AUDIT REPORT

Site Surveillance

Audit Services

FY2026

bclc

Table of Contents

Date: February 25, 2026

From: Rao Wandawasi, Director Audit Services

To Dan Beebe – Chief Operating Officer
Marie-Noelle Savoie – Chief Compliance Officer & VP Safer Play & Enterprise Integrity

Re: **SITE SURVEILLANCE AUDIT**

I. Introduction

In accordance with the FY26 Audit Plan presented to the Audit Committee, Audit Services conducted a review of BCLC's and Service Provider's surveillance operations and controls. The audit report is presented for information, discussion and incorporation of action plan items. For the issues identified, an "agreed upon action plan" has been developed in collaboration with management. These action plans are tracked by the Audit Services team for timely implementation. Any delays or non-execution of the action plan is compiled and presented to the Audit Committee periodically.

II. Objective and Scope

The objective of this audit was to assess both the current state and future direction of BCLC's and its Casino Service Providers' (CSPs) surveillance operations and controls. The review examined the effectiveness of existing policies, procedures, governance, and technology, as well as BCLC's ongoing and planned initiatives to strengthen surveillance capabilities.

A future-focused lens was applied to evaluate strategic planning, investment in emerging surveillance technologies, workforce development, and mechanisms for ensuring sustained compliance and operational resilience in a rapidly evolving regulatory and technological environment. In this regard, areas subject to Audit Services review included, but were not limited to the following:

A. <u>Current State Assessment of Surveillance Operations and Controls:</u>

a. **Policies and Procedures**: Reviewed existing surveillance policies and procedures to determine their adequacy and effectiveness

b. **Training and Experience**: Tested the current training programs and experience levels of CSP surveillance personnels to assess their readiness, qualifications, and alignment with BCLC expectations

c. **Surveillance Governance:** Examined the current governance structures overseeing surveillance activities, and how non-compliance is identified and addressed through corrective action

d. **Technology Investments**: Checked CSPs investments in surveillance technology, including modernization and innovation. Further, reviewed if BCLC is monitoring investment appropriateness

e. **Compliance Reports**: Reviewed the compliance division's surveillance reports (Asset Protection), focusing on their thoroughness, and effectiveness in identifying and addressing compliance risks

f. **Casino Walkthrough:** Conducted walkthroughs of casinos surveillance and operations to observe processes, verify controls, and assess the adherence to established policies and procedures.

B. <u>Future State Surveillance – Benchmarking and Adoption of Best Practices:</u>

a. **Benchmarking** – CSPs surveillance systems and standards against cutting-edge industry technologies

b. **Best Practices** – Assessed industry best practices in surveillance standards and technology

III. Executive Summary

Audit Services evaluated casino surveillance systems of CSPs, identifying critical areas requiring attention to strengthen governance, operational effectiveness, and regulatory compliance. Key points are listed below:

1. **Enforcement and Accountability:** Penalties by BCLC (coordinating with Regulators) to CSPs who have a pattern of surveillance non-compliance or limited responsiveness have monitory consequences and impact player experience (in case of site shutdown). BCLC leadership must decide on the importance of CSP compliance and weigh that against all other factors that impact operations and organizational financials. Additionally, Operational Services Agreement (OSA) limitations in terms of BCLC enforcement options for non-compliance is another restricting factor, which at times causes lackluster behaviour from CSPs towards compliance.
2. **Oversight:** BCLC may have to venture into areas (changes to the existing operating model) which the organization currently is not required to do per the established setup. The reason being gaps and concerns in these areas have far reaching effects. Further, the CSPs are struggling and unable to appropriately address them in a timely manner. Examples of these areas are:
    - Surveillance training programs
    - Whistleblower program review
    - Surveillance management teams experience
    - AI and its impact on surveillance technology
3. **IGCO and its Impact:** With new regulations coming into effect in April 2026 under IGCO, the compliance requirements, adherence expectations and consequential penalties for exceptions will all be tighter and stricter. This requires BCLC to work with CSPs to immediately identify all surveillance related exceptions, per the new regulations and address them. For those expected to be outstanding by April 2026, BCLC should immediately commence conversations with the regulator explaining when they will be addressed and the reason for the delay.
4. s. 17

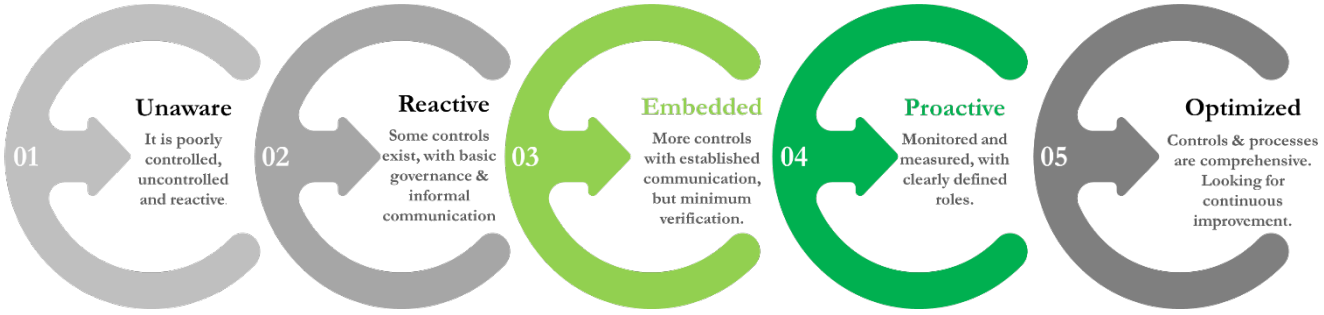
Essential Features of Modern Casino Surveillance

01	**Comprehensive, high-resolution coverage across all gaming and cash-handling areas.**
02	**Optimized mix of fixed and PTZ cameras for both wide visibility and rapid incident tracking.**
03	**HD recording standards (1080p+, 30 fps) to clearly capture gameplay and transactions.**
04	**Scalable storage supporting multi-week to 90-day retention and large data volumes.**
05	**Advanced analytics (facial recognition, behavioral alerts) to enhance real-time detection.**
06	**Redundant power, recording, and tamper-proof systems to ensure video integrity.**
07	**Strategic camera placement with Wide Dynamic Range /low-light technology for consistent visibility**
08	**Independent surveillance operations for unbiased oversight and data protection.**

s. 17

5. **Aspects to Consider Involving Policy:** At times, the current communication practice inadvertently causes gaps in CSP understanding and uneven application of key policies. Updates are not effectively disseminated internally within CSPs, leading to gaps in policy implementation. In addition, there is opportunity to strengthen policy understanding and actioning by CSPs by piloting new or revised surveillance policies with a select group before rollout.
6. **Training and CSP Surveillance Team Workforce:** Training programs could be tiered to reflect difference in site size, product offering and operational complexity. s. 15(1)

   BCLC could explore opportunities to support CSPs in their targeted training and mentorship to ensure roles and responsibilities are clearly understood.
7. **Compliance at the Core of Operational Excellence:** Currently, BCLCs surveillance maintenance schedule performed by the team within Compliance department is based on a frequency to meet bi-annual requirements. There should be consideration to revise the surveillance schedule based on the following factors: regular assessment, previous compliance report findings, and data analytics.



BCLC demonstrates characteristics consistent with a maturity rating of **2.5 (Reactive/Embedded).** The organization has established foundational surveillance controls, documented standards and policies, and formal governance structures through the OSA. There are regular management meetings with CSPs, periodic compliance reviews being conducted by the Asset Protection team, and established communication channels reflect an Embedded level of maturity where controls and processes are systematically in place across operations.

To mature to a Proactive level, BCLC should address the findings identified in this audit. By addressing these gaps BCLC can transition to a Proactive state with clearly defined roles, measured processes, and strengthened accountability in preparation for heightened regulatory scrutiny under IGCO.

Conclusion:

While foundational surveillance systems and framework are in place, enhancements and changes for further maturity are required in enforcement, governance, surveillance operating model with CSPs, and Compliance department. The IGCO transition in April 2026 will introduce heightened regulatory scrutiny, making enforcement of immediate action essential. Historical practice of only relying on warnings to CSPs could expose BCLC to potential financial and reputational damages.

IV. Details of Key Issues

1. Oversight that Drives Transparency and Boosts Compliance

By further stressing clear reporting structure, strengthening whistleblower programs, and addressing operational challenges, BCLC can foster a culture of transparency, accountability, and compliance. Proactive oversight and governance not only reduce regulatory and operational risks but also enhances stakeholder confidence, and positions BCLC as a trusted, resilient leader in the evolving gaming landscape.

Observation:

A. Strict Action Enforcement by BCLC and Acceptance of Accountability by CSP

a. Coordinate to Strictly Enforce the Consequences for Compliance Failures – For casino sites and CSP's who are repeat violators/offenders of key compliance and regulatory requirements, coordinating with Regulators there is a need to be stricter to reinforce importance of adherence to required standards. Historically, consequences for CSP non-compliance have been limited to warnings. These have not been effective in driving sustained corrective action.

- This approach does not address the root causes of non-compliance, as warnings are often not taken seriously by CSP management or frontline staff. This results in repeated issues.
- Further, limitations in OSA do not provide BCLC with many options, beyond "default notice" to drive CSP compliance.

Coordinating with Regulators, globally there are significant consequences for repeat offender non-compliant sites, including financial penalties, license suspensions, and operational restrictions.

b. IGCO Transition and Impacts to BCLC – Effective April 13, 2026, the newly formed Independent Gambling Control Office (IGCO) is replacing the Gaming Policy and Enforcement Branch (GPEB). IGCOs focus will be on gambling regulatory integrity and anti-money laundering, operating to reduce conflicts of interest and strengthen the objectivity of provincial oversight.

This will cause rigorous enforcement, greater oversight, increased scrutiny, and clearer expectations for compliance from CSPs, specific to surveillance. Further there are fines that can be imposed on CSPs up to $200K based on the nature of non-compliance. Under this environment, following is essential, as the regulations come into effect:

- Strengthening collaboration and ensuring mutual understanding of obligations will be key to mitigating the risks from the new regulatory regime.
- Finally, improve communication and address any gaps in coordination that could expose BCLC and CSPs to regulatory actions.

s. 15(1)

B. Evaluate CSP Safe Reporting Program and Promote Reporting Culture

a. Evaluate CSP Safe Reporting Program – BCLC could periodically review the CSP whistleblower (safe reporting) programs to ensure they are compliant, effective, and trusted by staff. A robust program provides clear, accessible reporting channels and sufficient resources to investigate concerns thoroughly. Critical issues were identified at a major CSP when a whistleblower raised the alarm.

Staff must feel confident reporting concerns without fear of retaliation, and that their issues will be addressed appropriately. An effective whistleblower program protects both BCLC and CSP while fostering a culture of integrity, transparency, and accountability.

b. Promote a Culture of Reporting and Transparency – CSP reporting practices continue to show inconsistencies. BCLC can play an important role in reinforcing the need for accurate, complete, and timely reporting.

- Several Surveillance Managers have begun promoting a proactive reporting culture by encouraging staff to document any event or incident they are unsure about, emphasizing transparency over uncertainty.
- One CSP has successfully implemented reporting incentives, yielding positive results.

Despite regular management meetings, reporting gaps persist. Sharing these practices more broadly across casino sites and CSPs may help improve consistency and elevate reporting standards.

C. s. 15(1)

Surveillance departments are redirecting resources from constant real-time observation to deeper investigative work, recognizing frauds/scams of 2025 often unfold in plain sight.

s. 15(1)

IMPACT:

As an industry, there is increased compliance risks, operational disruptions, and reputational exposure due to changes in the provincial regulatory framework, which will enforce stricter consequences for non-compliance. Gaps in reporting structures, weak whistleblower mechanisms, and s. 15(1) , potentially leading to inconsistent oversight.

Without proactive intervention, (in collaboration with Regulators), the entry of new owners and shifting industry standards could amplify these challenges, highlighting the need to address entrenched behaviours and strengthen governance across all sites.

AGREED UPON ACTION PLANS:

All aspects and gaps highlighted in this issue will be evaluated, discussed and necessary remedial measures developed. Subsequently, this will be discussed with CSPs and revised as necessary. Once accepted by both BCLC and CSPs, necessary changes in expected behaviour and practices will be incorporated and monitored to ensure continued adherence.

RESPONSIBLE PERSON:

SP&EI & Operations Divisions – March 31, 2027

2. Further Improve Foundation Aspects for Operational Excellence

Strengthening policy consistency, clarifying key terms, and enhancing document accessibility and operational coordination lays the groundwork for operational excellence. This approach ensures uniform application of surveillance standards, reinforces accountability, and promotes efficient and compliant operations organization-wide.

OBSERVATION:

A. Aspects Impeding Appropriate Application of Standards/Policies

a. Better Communication of Standard Changes Between BCLC and CSPs – Communication of surveillance standards and any other procedural changes to them currently exists between BCLC and CSPs but could be improved. At times, the current communication practice inadvertently causes gaps in CSP understanding and uneven application of key policies. Updates are sometimes not effectively disseminated leading to gaps in policy implementation.

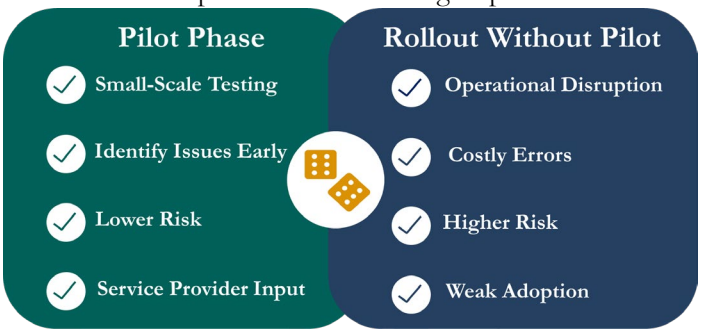
s. 15(1)

b. Inconsistent Application of Policies and Prodecures – Instances of non-compliance with established surveillance policies by both CSPs and BCLC were noted. Compliance is always required, but more so in the new IGCO environment. Compliance is not a nice to have, but a must-have element. Couple of examples of non-compliance are:

s. 15(1)

Organizations with active policy monitoring and enforcement see 40% reduction in non-compliance. – KPMG

c. Pilot Testing and Feedback Prior to Full Implementation/Rollout of Policy – There is an opportunity to strengthen policy implementation by piloting new surveillance policies with a select group of CSPs before full rollout. Testing on a smaller scale allows for feedback on clarity, practicality, and operational impact, ensuring policies are effective and achievable. This approach promotes collaboration, reduces the risk of misinterpretation or compliance issues, and supports smoother adoption across all sites.



B. Policy and Document Challenges

a. Issues within the Policy – In discussion with multiple CSP personnel, a few aspects were presented as concernes and practical challenges specific to policies, which if addressed will better aid in policy adherence and potentially mitigate non-compliance concerns. Examples of these CSP concerns specific to policies are:

- Certain aspects within the surveillance policies are fragmented, sometimes ambiguous, and open to interpretation, resulting in inconsistent practices across sites.
- Specific terms within the surveillance policy and standard are subjective. This results in inconsistent interpretation by CSPs.

Organizations with clear, standardized policies are 3X more likely to consistently comply. -Deloitte

Service Providers have occasionally developed their own manuals to fill procedural gaps, increasing the risk of non-compliance, inconsistent incident responses, and lapses in surveillance coverage or evidence handling. BCLC is currently updating its surveillance standards to address these issues.

s. 15(1)

b. Limited Accessibility and Search Functionality – Key surveillance policies and standards are difficult to locate within the current PDF due to limited search functionality. This impedes operational efficiency, and can result in inconsistent application across sites, particularly during time-sensitive surveillance activities.

Further, in the current setup, there is no interactive table of contents or searchable index, which can be leveraged to search frequently referenced terms. These could result in BCLC and CSP personnel unable to quickly and accurately access relevant guidance, support timely decision-making, and strengthen uniform operational practices and adherence to standards across all surveillance sites.

Improved documentation search can boost knowledge-worker efficiency by 20-35% - IDC Information Worker Productivity Study

IMPACT:

Hard-to-navigate surveillance policies, coupled with gaps in communication and operational coordination, could lead to inconsistent practices, misinterpretation, and alternate manuals developed by Service Providers. Limited document accessibility, inadequate dissemination of updates, non-compliance with procedures, and lack of consultation have increased regulatory risk.

AGREED UPON ACTION PLANS:

The standards are currently being reviewed and updated as required to streamline the overall setup. All points highlighted within this issue will be noted and appropriately considered as the updates to the standards are finalized.

This should address all concerns that are emphasized.

RESPONSIBLE PERSON:

SP&EI & Operations Divisions – March 31, 2027

3. BUILDING A SKILLED, SUPPORTED, AND MOTIVATED WORKFORCE

Investing in a skilled, supported, and motivated workforce enhances compliance, strengthens operational performance, and fosters a culture of accountability. This enables the organization to manage risks effectively and maintain consistent excellence across all Service Provider sites.

OBSERVATION:

A. Training Program Design and Relevance

a. Training Levels by Site Category – Training programs could be further tiered to reflect differences in site size, product offerings, and operational complexity. For example:

- Sites with table games require both CSO 1 and CSO 2 training
- Locations without table games only require the foundational CSO 1 course.

This variation demonstrates the need for training requirements that align with the specific demands of each operation location.

Urban casinos could typically face organized crime, complex fraud schemes, and large-scale incidents, while rural sites possibly encounter smaller thefts, insider misconduct, and low-tech cheating. These differing risk environments, transaction volumes, and process complexities reinforce the need for tailored surveillance training that addresses crime types, incident response, and reporting expectations.

A tiered approach supported by ongoing collaboration with CSPs would enable more targeted instruction, ensure operational alignment, and better equip staff with skills appropriate to their site.

Example

One larger urban Service Provider distributes their own test specific to their facility and their policies based on the incidents they encounter. New candidates have 3 months to train and study and must reach a 75% mark or must redo this test.

s. 15(1)

B. Assess CSPs Surveillance Teams Workforce Capability and Readiness – BCLC's Role

BCLC currently has no role or responsibility but could consider looking into the following to support/help CSPs which in long term will aid BCLC and the surveillance programs at site. (Obviously, BCLC resource availability is a key aspect to be considered).

- CSP staff capabilities vary significantly, particularly within surveillance leadership. BCLC could support in the assessment of their experience gaps and identify opportunities for targeted training and mentorship to ensure roles, responsibilities, and expectations are clearly understood.
- Focused development initiatives can help address factors contributing to turnover such as insufficient preparedness, and strained staff–management relationships at certain sites.
- There is also an opportunity for BCLC to highlight high-performing locations and facilitate the sharing of effective practices.

Example

One major Service Provider has enhanced training for its staff members but also offer competitive pay with annual pay raises, allow for flexibility in shifts and have given monetary incentives for catching incidents of theft. In many cases staff only move on for better opportunities and promotion.

IMPACT:

Poorly trained surveillance teams and weak management can have severe consequences, including undetected cheating, collusion, or internal theft, incomplete incident reporting, and exposure to regulatory penalties. The absence of accountability further fosters a complacent culture, erodes morale, and damages the casino's reputation, creating operational inefficiencies and long-term profitability challenges. Negative perceptions can spread quickly through social media and word of mouth, reducing customer loyalty, deterring high-value players, and impacting vendor or investor confidence.

With the upcoming implementation of the IGCO enforcing stricter controls in British Columbia, maintaining strong leadership, skilled staff, and rigorous compliance is critical to protect the casino's operations, profitability, and brand credibility.

AGREED UPON ACTION PLANS:

Current operating model of BCLC does not involve supporting or assessing CSPs surveillance staff specific to their training, and succession planning. However, given the continued challenges and issues faced at CSP sites specific to surveillance concerns, all issued highlighted in this issue will be considered and any changes to the methodology that could better address this challenge will be discussed and actioned as needed.

RESPONSIBLE PERSON:

SP&EI & Operations Divisions – March 31, 2027

4. COMPLIANCE DEPARTMENT AT THE CORE OF OPERATIONAL EXCELLENCE

Enhancing visibility and controls across operations provides a foundation for stronger oversight, proactive risk management, and consistent compliance. Further, sufficient investment in surveillance technology and resources within the Compliance team will improve monitoring and develop a robust control mechanism. This comprehensive approach not only mitigates regulatory and operational risks but also strengthens decision-making and supports long-term organizational resilience and performance.

OBSERVATION:

A. Determine Revision of Maintenance Schedules based on Risk and Operational Needs

The Compliance and Corporate Security/Asset Protection teams are under increasing pressure due to escalating casino site issues and rapid growth in tasks, particularly new-to-industry employees and organizations. These teams now deliver:

- Training on surveillance, compliance, and security awareness
- Education on ethical conduct and risk behaviours, and
- Onboarding support for new organizations.

With the IGCO effective April 13, 2026, regulatory scrutiny will intensify. Without additional resources, the teams risk being overextended and unable to:

- Deliver consistent compliance monitoring
- Provide timely training and onboarding, and
- Maintain required oversight under the new regulatory framework.

Current capacity may be insufficient to meet growing operational and regulatory demands, risking long-term compliance effectiveness and organizational readiness.

B. CSPs to Invest in and Optimize Surveillance

Optimizing surveillance operations requires investment in quality technology that provides clear imaging and reliable monitoring. Reviewing CSP component plans can identify essential functionalities to ensure consistency across sites, as core system features like alerts and predictive tools are often variably activated.

CSPs should be encouraged to evaluate the cost-effectiveness of system upgrades through formal cost-benefit analyses, with BCLC providing guidance and oversight.

As highlighted in the February 2025 Summary Report, the Asset Protection team is well-positioned to collaborate with CSP surveillance leadership to educate staff on available technologies, identify system gaps, and recommend strategic upgrades. These efforts ensure that the surveillance systems remain robust and effective, extending beyond mere compliance obligations to support overall operational excellence.

s. 15(1)

C. Review Compliance Team's Resourcing

There are a few aspects occuring simultaneously, that are impacting the Compliance team and its resourcing. They are:

- With nature and extent of issues and gaps at the casino sites, there is greater ask to the Compliance team in terms of repeated testing, reviews, etc.
- The current Regulator (GPEB) have stated and expect the Compliance team to have greater presence at the casino sites and perform more tests/reviews.
- With IGCO coming into effect April 13, 2026, there will be a greater demand of Compliance teams' expertise and resources to perform additional work due to greater scrutiny.

Under these circumstances, the Asset Protection team's staffing within the Compliance department may be challenged to support comprehensive compliance monitoring, implementation of new initiatives, and ongoing engagement with CSPs.

D. Ongoing Monitoring of Succession Planning – Asset Protection Team

The Asset Protection team has succession planning mechanisms in place to support operational continuity and preserve institutional knowledge. Given the team's small size and the depth of experience within the group, continued oversight and regular review of succession planning is critical to maintain business continuity in the event of personnel transitions or retirements.

Sustaining a structured succession approach through ongoing documentation of key processes, identification of potential successors, and targeted development will help ensure long-term resilience and continuity.

IMPACT:

Failure to optimize maintenance schedules and efficiency may result in lower asset reliability, increased repair costs, and higher operational expenses. Likewise, delayed or insufficient investment in surveillance technology by CSPs could weaken the long-term effectiveness of site surveillance.

From a compliance perspective, sufficient resourcing is essential, particularly in a changing regulatory environment. There is also an ongoing succession and knowledge retention risk within the Asset Protection team due to its small size and specialized expertise.

AGREED UPON ACTION PLANS:

Items highlighted specific to the Asset Protection team within the Compliance department will be reviewed, and appropriate remedial actions will be taken. Relevant departments will also work with the CSPs to discuss necessary investments in surveillance equipment to enhance overall site security.

RESPONSIBLE PERSON:

SP&EI & Operations Divisions – March 31, 2027

V. Other Opportunities

The other opportunities section is provided for management's consideration. Audit Services will not be following up with management to determine if the aspects highlighted in the other opportunities section have been implemented. It is left to management's discretion.

s. 17

s. 17

Appendix I – Best Practices Surveillance Systems in Casinos

In today's casino environment, a best practice surveillance system is far more than rows of cameras. It is an integrated, high resolution, intelligently managed "eye in the sky" tailored to the unique risks and regulatory demands of gaming operations. Modern surveillance systems have become indispensable, with the global casino surveillance market valued at US $1.9 billion in 2024 and is projected to nearly double over the coming years as operators increasingly adopt IP based cameras, advanced analytics, and robust storage.

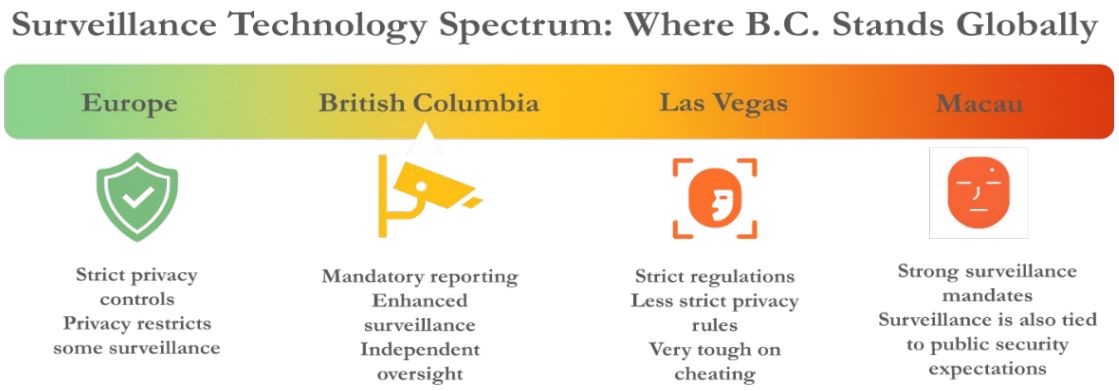
Coverage: At the core is comprehensive coverage. Every gaming table, cashier cage, drop box, slot machine bank, count room, entrances and exits, and back of house area is carefully mapped and monitored. 60 to 70% of cameras tend to be fixed, providing constant wide-angle surveillance, while 30 to 40% are PTZ (pan tilt zoom) cameras to allow real time tracking and dynamic review when suspicious behavior occurs. In large casinos, including major resorts, it is not unusual to find thousands of cameras, with some venues reportedly exceeding 2,000 devices, covering hundreds of thousands of square feet.

Quality of Image: Image quality and recording parameters are equally critical. Best practice calls for high-definition video, often 1080p or higher, with recordings at 30 frames per second (fps) across high liability areas such as tables, cages, and count rooms. For zones with high motion, such as gaming tables or slot floors, some casinos configure cameras for higher frame rate or motion triggered capture to ensure card deals, chip movements, and other critical details are clearly visible.

Storage: Because gaming floors generate vast volumes of video, operating around the clock, a robust storage and retention architecture is essential. Leading systems employ scalable, enterprise grade storage designed to retain footage for extended periods. Many casinos retain video for multiple weeks by default, and for certain high-risk zones or after detected incidents, retention can extend to 90 days or more. Some properties manage multiple petabytes of surveillance data annually as operations scale.

Analytics: Beyond raw video, modern casinos increasingly deploy analytics and intelligent detection tools. These may include facial recognition for excluded patrons, behavioural analytics to detect patterns such as unusual betting or dealer anomalies, and automated alerts that surface suspicious events in real time. In 2023, more than 70% of new surveillance deployments incorporated IP cameras with high resolution, and many included AI features, a trend reshaping how casinos balance human observation with automated monitoring.

In summary, a best practice casino surveillance system consists of a dense network of high-resolution cameras, intelligent analytics, enterprise level storage, strong redundancy, and disciplined operational oversight. Such systems provide both real time protection and critical forensic capability, supporting integrity, regulatory compliance, and long-term operational resilience in the gaming industry.



Distribution List

Sandy Austin
Bal Bamra
Pat Davis
Mark Goldberg
Alan Kerr
Natasha Questel
Kevin Sweeney

Communications

Laura Piva-Babcock

Audit Team

Karen Gaia-Maretta
Raj Lidder
Meetul Patel
Darryl Tateishi
Rao Wandawasi

AUDIT REPORT

Artificial Intelligence (AI) Systems Review

Audit Services

FY2026

bclc

Table of Contents

Date: February 26, 2026

From: Rao Wandawasi, Director Audit Services

To Mark Goldberg, Chief Information Officer and VP, Business Technology

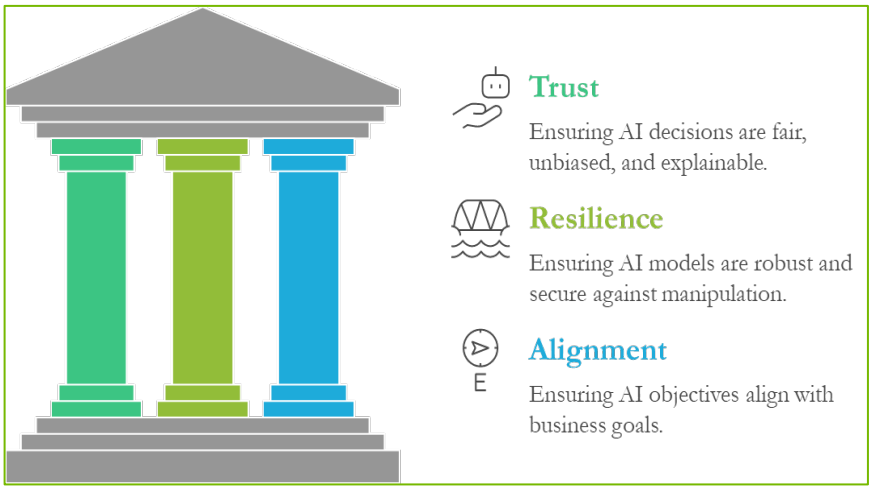
Re: **Artificial Intelligence Systems Review**

I. Introduction

Artificial Intelligence (AI) is no longer a frontier technology but becoming a core tool for Canadian business in recent years. Companies are increasingly relying on AI to drive critical decisions and solve specific problems – from personalizing customer interactions, optimizing supply chains to information strategic investments.

Various business functions in BCLC are also experimenting with AI tools to strive for growth and efficiency. As of October 2025, there are 54 AI powered tools approved by the company. For example, the Digital Employee Workspace team has launched [s. 15(1)(l)] , an AI-powered chatbot that helps employees access answers to BCLC corporate policy questions. Another example is Enterprise Data Office using [s. 15(1)(l)] for Data Scientists and Software Developers to create Machine Learning model, automating the data classification process.

With this great AI power comes a new type of responsibility and challenges, and they could have major consequences for an organization. For example, privacy violation, security threats, intellectual property and reputation damage.



Currently, Canada has not issued any clear regulatory guidance or standards, in addition, AI systems are a dynamic technology moving faster than regulations. The rationale for conducting this audit is not merely checking a compliance box, but to future-proof the organization and to help build a foundation of Trust, Resilience and Alignment for the AI ecosystem.

Looking ahead, regulatory scrutiny around AI is intensifying globally. By proactively auditing our AI setup today, we are not just mitigating current risks but building a scalable and responsible framework for the AI-driven innovations of tomorrow. This audit is a critical step in ensuring that the use of AI remains a sustainable competitive advantage, fostering trust among our customers, employees, and stakeholders for years to come.

II. Scope, Objectives and Methodology

A. Scope

The scope of this review was limited to BCLC's internal systems and processes, excluding Casino Service Providers (CSP), Lottery Retailers and iGaming vendor platform. A determination will be made later if another phase of this audit is to be performed reviewing the AI landscape of all BCLC third-party vendors and CSPs.

B. Objectives

The review took a future-focused approach by assessing BCLC's plan and foundational steps, to acquire, monitor, and manage AI technologies to enable the effective and responsible use of AI. Accordingly, the objectives include:

a. **Preparing AI adaption for now and the future:** Assess the organization's actions to establish the foundation for a secure, well-governed, and trustworthy AI environment currently and into the future. This includes evaluating responsible AI principles, AI uses case inventory, AI risk taxonomy, and AI intake and tiering.

b. **Integration of AI across BCLC:** Evaluate how AI capabilities are positioned to align with the strategic priorities and support delivery of business value. Determine if AI is embedded as part of the broader enterprise rather than functioning as a standalone activity.

c. **Traceability, transparency, and explainability of AI systems:** Assess BCLC's preparedness for responsible use of AI tools by examining how the organization ensures key principles of explainability, transparency, and traceability, are addressed through vendor agreements and documentation.

d. **Future compliance readiness and capability building:** Understand BCLC's alignment with legal, privacy and any future regulatory requirements for AI. Further explore opportunities to build coordinated program where all parties, including the second line (ERMS, Compliance, Legal) and third line (Audit Services), work together to ensure continuous compliance and meeting of regulatory entitites external audit requirements.

e. **Strategic opportunities for AI enablement:** Review BCLC's approach to identify AI tools that support the strategic roadmap and are scalable to effectively transform our business.

C. Methodology

The review used ISACA AI Audit Tool Kit to facilitate assessment of AI systems governance, security and compliance. The kit synthesized requirements from major frameworks and regulations into a single resource and has 22 control families. Based on the specific audit objectives, Audit Services mapped and aligned all relevant controls across key domains including:

a. **Governance & Strategy:** involves overarching governance and strategic planning of AI initiatives

b. **Ethical AI & Accountability:** encompasses ethical considerations and accountability of AI systems

c. **Training & Awareness:** includes enhancing AI literacy initiatives

d. **AI Bias Mitigation & Fairness:** dedicated to identifying and mitigating biases in AI systems to ensure fair and unbiased decision-making processes

e. **AI Data Privacy and Rights:** addresses the protection of data in AI systems, emphasizing personal data rights and compliance with data protection laws

f. **AI Life Cycle Management:** covers the entire life of AI systems, from development to maintenance

g. **External Components & Supply Chain Governance:** manages and secures external vendors and supply chains of AI systems

h. **Data Protection:** focuses on safeguarding AI system data against unauthorized access and breaches

i. **Legal & Regulatory:** reviews legal/regulatory asepects of AI including compliance and prohibited use cases

j. **Cybersecurity & Resilience:** protects AI systems from cyber threats through secure design, threat monitoring, and incident response.

The findings and recommendations are designed to guide strategic decision-making, close readiness gaps and build a robust foundation for the secure and value-driven integration of AI across the enterprise.

III. Executive Summary

A. Introduction

The review recognizes that BCLC has made notable progress in its adoption of AI, establishing a strong foundation for governance and future innovation. There are numerous positives, a few examples are listed below:

a. Various business functions are actively pursing both buy and build AI initiatives tailored to specific customer needs.

b. The partnership with AnthemXT to create an internal innovation hub has been set up since November 2024 to support AI initiatives.

c. The organization has taken critical first steps in AI governance by completing an initial risk assessment, forming an AI Steering Committee and drafting a policy for upcoming Board approval.

d. Customer Support Center (CSC) has developed tangible business value and increased work productivity through AI and have implemented governance controls within the department.

e. Enterprise Data Office is implementing an Enterprise Data Strategy and adopted AI-powered governance and catalog tools such as s. 15(1)(l) which uses machine learning to suggest data classification.

B. Key Findings

As the organization progresses from initial experimentation to broader implementation, the audit identified certain key opportunities to strengthen the framework, support responsible and effective scaling of AI initiatives:

a. Strategy and Governance – While AI is referenced in the Enterprise Data Strategy, it lacks integration into core corporate strategy and priorities. Further, it lacks a unified governance framework that does not encompass the authority or controls for effective oversight.

b. Ethics and Responsible AI – An enforceable ethical and responsible AI policy and clear standards are currently non-existant, leading to ambiguity for employees and gaps in permissible use.

c. Accountability and Oversight – Clear AI ownership and robust technical governance process is currently not in place. This results in initiatives occurring randomly rather than being coordinated, and a lack of enterprise-wide oversight and accountability for AI tool usage and risks.

d. AI Literacy and Change Management – While BCLC is integrating AI into its operations, that could affect workflows, decision making and customer interactions. The limited AI literacy among employees and lack of a structured approach to manage changes may suppress the innovation.

e. Data Foundation, Architecture and Information Security – Although strong progress in data governance and cybersecurity have been made, challenges remain in migrating legacy systems, aligning data definitions, and enabling AI-driven insight. Data needs have evolved from siloed business-unit analysis to enterprise-wide insights. However, systems often do not align with these organizational needs.

f. Vendor and Third-Party Mangement – High dependency on vendors with limited transparency into their AI models is noted. Vendor contracts need to evolve to keep pace with evolving AI landscape.

g. Culture of Experiementation – Need to build a culture where experimentation is encouraged, and failure is treated as a learning opportunity. Leaders should support this by setting clear boundaries, reducting fear of mistakes, and recognizing effort not just success.

C. Critical Action Items to Consider

Based on the nature of findings, few key action items are listed for management's consideration:

a. Recognize AI is a Technology Enabler: AI is not a separate initiative, but a technology enabler that must be integrated into the corporate strategy

b. Define Acceptable Risk: Establish acceptable risk thresholds to compete effectively, while also understanding the risk of inaction

c. AI Framework must be Dynamic: Governance and strategy need to always be aligned with emerging regulation and technological shifts

d. Governance must be Dynamic: Governance must be risk-based and agile to avoid hampering innovation and should support catching up with rapid developments

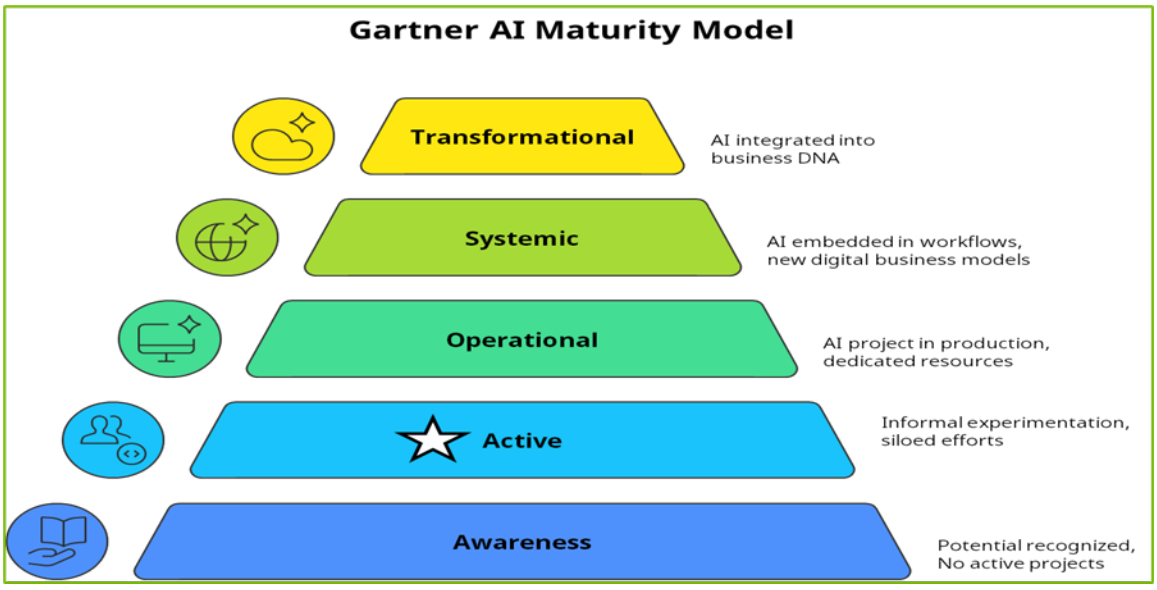
e. Executive Support and Board Engagement are Critical Enablers: Executive support and Board oversight help ensure alignment, accountability, and funding for key initiatives

f. Change Management: Proactive change management is critical for adoption, mitigate resistence and fully realize the value of AI investment

g. Workforce Planning: There is a pressing need for comprehensive reskilling and upskilling, since AI will inevitably automate tasks, augment capabilities and change processes.

D. Maturity Assessment

Audit Services performed an evaluation against the Gartner AI Maturity Model which revealed that BCLC's overall framework and process maturity level is at **2 – Active**. This score means that the company has informal experimentation with AI, including proof of concept and pilot projects; however, efforts are often siloed and not yet standardized across the organization.



To harness AI's full potential, BCLC must transition from scattered initiatives to a governed, corporate strategy oriented, business value focused AI program. It should be anchored to strategic outcomes, enforced by tiered controls, and supported by accurate data, strong security, and skilled workforce to scale safely and productively.

IV. Details of Key Issues

1. AI Strategy, Governance and Ethical Responsibility – Requires Further Streamlining

Building an enterprise-wide AI strategy is not just about adopting technology, it is about shaping the future of how the organization thinks, operates, and innovates. By laying a strong foundation today, the company creates the blueprint for responsible, scalable, and value-driven AI that empowers every business unit. Governance becomes the cornerstone of trust, ensuring that AI decisions are ethical, transparent, and aligned with the organization's mission.

Observations:

BCLC has been experimenting AI tools across various business functions and some initiatives are delivering value. However, an enterprise-wide AI strategy, which informs operating model and aligns with corporate strategic goals, is not established.

A. AI Strategic Integration

AI strategy should focus on "why" (the problem) before the "how" (technology)

a. The Corporate Strategy was developed before the recent acceleration of AI. AI is not fully woven into all aspects of the strategy, which reduces its visibility as a tranformative capability. AI is referenced in the Corporate Data and Analytics Strategy but not deeply embedded across other strategic priorities.

b. AI is not positioned as a core driver of business objectives, resulting in limited alignment with enterprise-level goals. There is no clear definition of what the organization aims to transform through AI.

c. AI is treated as a technical tool rather than a business enabler, creating a disconnect between tactical implementation and enterprise-level objectives.

Failing to have an AI strategy is viewed as a choice to be unprepared for a fundamental shift.

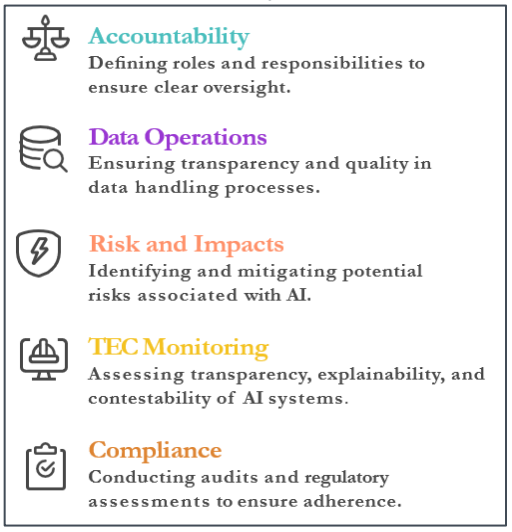
B. AI Governance

a. s. 15(1)(l)

b. A tiered governance approach can balance stronger oversight for high-risk, "crown jewel" areas and with lighter controls for low-risk cases to manage AI initiatives.

c. AI oversight is currently distributed across multiple governance and review bodies. While this provides controls, a more centralized coordination model for AI-specific initiatives could improve efficiency and clarity.

AI Governance – Key Components



C. Ethical Framework Gaps

Ethical principles must be translated into concrete practices to ensure responsible AI. This requires embedding fairness, transparency, and accountability into the entire AI lifecycle.

> Responsible AI is not an add-on, but a core component of integrity and trust.

a. BCLC is not currently equipped with a documented AI ethical framework or a dedicated group responsible for enforcing ethical standards. Accountability is undefined, if AI systems make incorrect or harmful decisions.

b. Ethical decision making is unclear for sensitive behavioral patterns (e.g. identifying high-risk players). Without clear ethical guidelines, decisions about how AI generated insights are used (e.g. personalization vs. player protection) remains ambiguous.

c. Users may assume AI will automatically change outcomes (AI misconception), but AI only provides insights. Human interpretation and ethical action remain essential.

d. Fairness assessments and explainable AI practices have not been systematically applied.

D. Policy and Standards

a. BCLC currently relies on an optional AI guideline rather than a formal, enforceable policy and standards, resulting in fragmented understanding and inconsistent practices across teams. Unlike other domains such as data privacy (Personal Informaton Protection and Electronic Documents Act (PIPEDA) and BC's Freedom of Information and Protection of Privacy Act (FIPPA)), there are currently no defined technical standards for AI usage.

b. Security monitoring shows usage of non-approved AI tools, this may reflect personal use for efficiency or convenience, and this should be addressed through cybersecurity policy alignment and AI literacy assessment. For example, in October 2025 the top two AI tools used by employees are the nonapproved and informal tools – Grammarly and ChatGPT. The approved s. 15(1)(l) was third in the list of most used tools.

c. Existing policies provide a baseline for AI usage. However, the current policy creation approach is slow and rigid, making it unsuitable for the rapidly evolving AI landscape. Trying to create a perfect policy upfront can make it outdated before it is used as AI is rapidly changing.

d. Approved AI tool list or allow-listing[1] process is not widely available or communicated to the employees.

IMPACT:

The absence of a mature enterprise-wide AI strategy and governance framework expose the organization to operational inefficiencies, compliance risks, and missed opportunities. AI initiatives may fail to deliver consistent value or align with business objectives.

[1] An allow-listing process is a security and governance control that specifies an approved list of entities, such as AI models, data sources, software libraries or users, that are explicitly permitted to operate within a defined environment. Everything else is denied by default.

PROPOSED ACTION PLANS:

Establish a coordinated approach to the governance and use of AI across BCLC. This will include establishing a cross functional AI Steering Committee and including a strategic AI lens into existing strategy and governance processes. Example: CAIR, Architecture Review Board.

RESPONSIBLE PERSON:

BT Division with Support from all other Divisions – March 31, 2027

2. Gaps in Accountability, Initiatives Prioritization and Review Process

Clear, defined ownership for AI systems, from conception to decommissioning, is the cornerstone of effective accountability. Oversight should be multi-layered, combining a central governance body with technical reviews and ongoing monitoring. This requires formally assigned roles, documented decision rights, and proactive processes to assess models for fairness, explainability, and drift throughout their lifecycle.

Observations:

A. Ownership and Accountability – BCLC Leadership and Board

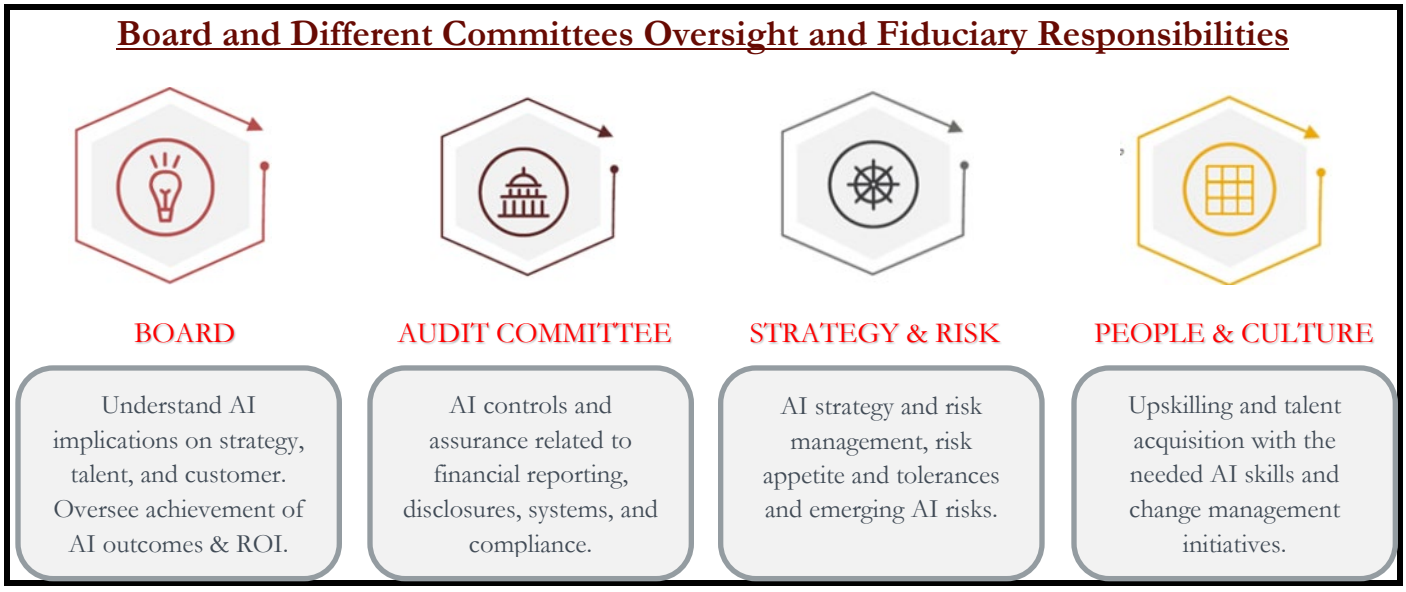
The organization has not established a clear ownership model for AI initiatives. Several teams contribute to AI initiatives; however, accountability is dispersed, creating a decentralized landscape. A culture of ownership and accountability is required to ensure responsible and effective AI adoption. Few options to consider by business from an AI accountability perspective are:

a. An integrated C-suite approach, supported by Board oversight, to set direction and approve AI strategy.

b. Dedicated resource to drive AI innovation and build governance.

c. Clear accountability at the business and technical levels for AI development, deployment, and monitoring, supported by second-line challenge function.

AI governance is a shared responsibility across the entire Board, with different Committees playing distinct roles to ensure oversight, risk management, and strategic alignment.



B. AI Steering Committee

a. AI Steering Committee was established in September 2025 to improve visibility and coordination. The Committee is performing well but is still in its early stage of operation.

b. Terms of Reference outlines a mandate to develop an enterprise-wide AI governance framework, but this document is not finalized. Further decision-making authority and governance process for the Committee is yet to be defined.

c. The Committee lacks representation from Operations, Social Purpose, Enterprise Risk Management (ERMS), and Legal teams. These teams provide critical perspectives on ethical considerations, regulatory compliance and operational alignment.

d. Multiple teams (e.g. Gaming, Marketing, Customer Support) leverage AI, but they operate independently with distinct objectives. This could result in conflicting outcomes with ethical blind spots. For example, AI generated insight is aimed at pursuing revenue but undermines player safety.

C. Use Case Prioritization

a. There is no structured enterprise-wide approach to identify and prioritize AI use cases and validate they align with organizational goals and would delivery measurable values. It could be challenging to trace AI initiatives alignment (if any) to enterprise objectives.

b. Use case assessments are not consistently performed with involvement from business teams and second-line functions (ERMS, Privacy, Legal, and Compliance), limiting visibility into potential business and compliance risk.

c. Existing inventory[2] lack standardised criteria for priortization, risk assessment or lifecyle management.

d. A structured process for ongoing monitoring of AI model post-implementation is not established.

D. AI Initiative Review Process

The Compliance Assessment Intake Review (CAIR) process has been established as a formal review and approve workflow for AI related initiatives. While existing technical governance processes are leveraged for AI initiatives, they were designed for traditional software and are not fully optimized for the dynamic and iterative nature of AI. As a result, there is no formal evaluation of fairness, bias detection, or model transparency. Following issues exist within this process:

In the CAIR process – there is no technical review focused on ethical AI considerations.

a. It lacks technical skill (data analysts or data scientists) assessments.

b. s. 15(1)(l)

c. All new AI use cases required full CAIR approval. Even the low-cost trials, like the proof-of-concept. This introduces delays and negatively impacts timely experimentation.

d. No automated capability exists for real-time monitoring of AI model performance or drift.

[2] Current Data CoE Knowledge Base maintains an inventory of AI-Buy Inventory & AI/ML Build – Use Case Library in s. 15(1)(l)

IMPACT:

This could increase risk of biased or flawed decision making and difficulty in ensuring accountability and transparency. Fragmented usage across departments reduces efficiency, creates duplication of effort and limits leveraging AI in a coordinated and strategic manner.

PROPOSED ACTION PLANS:

To ensure we do not slow down innovation and creativity the focus of our response will be to create centralized visibility of AI activity at BCLC via the AI Steering Committee and insure the appropriate integration into existing approval and governance processes. Example: CAIR, Architecture Review Board.

RESPONSIBLE PERSON:

BT Division with Support from all other Divisions – March 31, 2027

3. Opportunity to Further Strengthen Organizational Culture and Change Management Specific to AI Deployment

Optimizing AI capabilities is not just a technical challenge, it's a leadership priority. Successful AI adoption requires proactive change management to address skill gaps, redefine workflows and build trust. As AI becomes more embedded in operations and decision-making, BCLC must ensure its people, processes, and partnerships are ready. This means building AI literacy across all levels and aligning tools with business needs.

Observations:

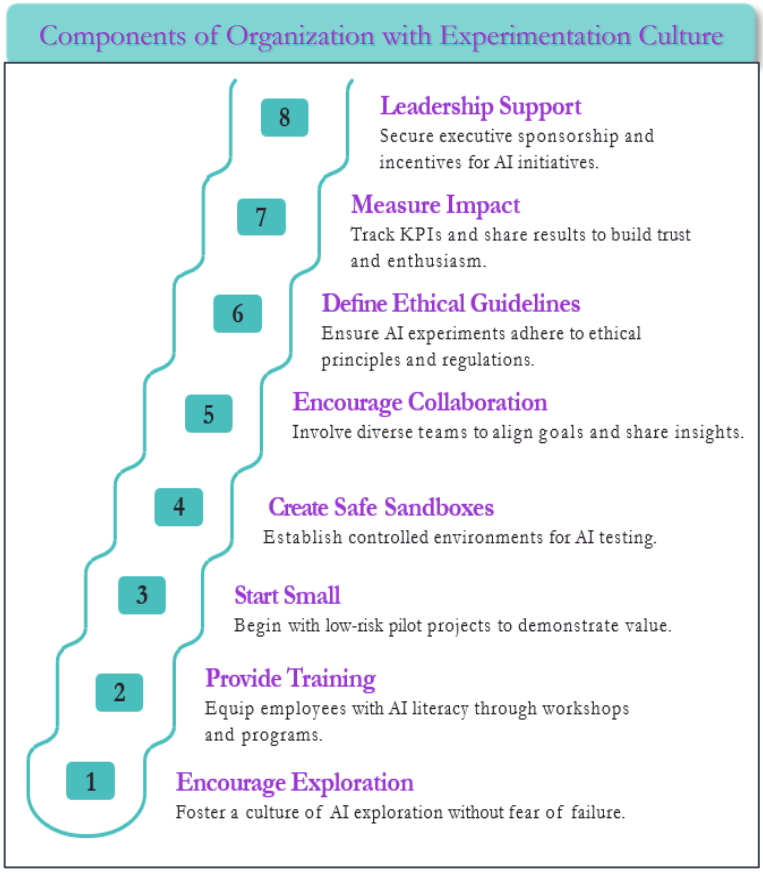
A. Culture of Experimentation

The organization needs to integrate AI into everyday work and foster a culture of experimentation. Under the current setup, following challenges remain organization wide:

a. Need to build a culture where experimentation is encouraged, and failure is treated as a learning opportunity. Leaders should support this by setting clear boundaries, reducing fear of mistakes, and recognizing effort not just success.

b. In fast-moving markets such as iGaming, where personalization and innovation are critical, slow adaption increases the risk of falling behind private-sector competitors who operate with fewer regulatory constraints and potentially greater agility.

c. AI adaption cannot be driven solely by BT. It must be embedded across the organization with clear outcomes, empowered users, and redesigned workflows.



d. Existing governance structures prioritize risk management and compliance. AI-specific governance needs to balance innovation with oversight as AI adaptation expands.

e. There is fragmentated AI knowledge across organization with no dedicated resource capturing lessons learned across AI projects. Successful initiatives like CSC call center transformation are not consistently shared, limiting visibility and cross-functional learning.

f. Limited availability of secure sandbox environments constrains employees' ability to safely explore and test AI use cases during regular work activities. This leads to increasing experimentation on personal devices, which may inhibit innovation and slow organizational learning.

Real AI transformation is not about technology. It is about culture, how we work, how we think and how we deliver value.

B. AI Literacy and Training

Interest in AI continues to grow; however, the knowledge required to use it responsibly and effectively is limited and not widespread.

a. Some educational efforts have been made, including training on s. 15(1)(l) , but these initiatives lack continuous updates on evolving AI innovations and have not been formally integrated into a broader learning strategy. Continuous reinforcement and targeted education will help sustain and deepen AI literacy as tools and use cases mature.

> Organizations need to help employees transition to an AI-centric workplace to ensure no one is left behind.

b. Employees lack clarity on how third-party AI applications operate, process data, and generate decisions. This gap in understanding further extends to both responsible use, and limited awareness of approved AI-enabled tools.

c. A level of caution for AI use exists, across the organization. This apprehension may be shaped by external narratives, including media reports of organizations facing reputional damage due to unchecked AI outputs. This fear of the unknown may impact strategic momentum.

d. Given AI is still relataively new, the progress and maturity of organization specific to AI adoption should be assessed and shared with employees. This will provide a basis and required knowledge on organizational progress.

   (There are different tools available, one example being Mitre AI Maturity Model. It provides a balanced structure measured across six-pillars and focused on areas key for BCLC namely – Ethicial Use, Strategy & Resources, Organization, Data, Technology Enablers and Performance & Application. Mitre provides an adaptable, scalable approach for both early-stage and advanced AI adoption.)

C. Change Management's Role in AI Initiatives

BCLC has an established Change Management team that supports programs and projects through structured methodology and is also engaged in developing self service tools and templates for smaller initiatives.

a. Currently, for AI related initiatives (except for s. 15(1)(l)), the Change Management team has not been actively engaged.

b. There is no direction on when Change Management should be involved in AI initiatives. Awareness of Change Management team's role and when and how business units should utilize their expertise appears limited across the organization.

> Successful digital transformation encompasses 10% technology and 90% change management.

As a result, significant AI-driven projects and changes appear to proceed without appropriate change mangement support.

IMPACT:

Without a foundational understanding of AI, employees may unintentionally misuse tools or misinterpret outputs, leading to operational inefficiencies or reputational harm. The absence of formal training and limited awareness of guidelines means that responsible use is not consistently practiced, as AI tools are more embedded in daily workflows.

Limited awareness of Change Management function for AI-related initiatives increases the possibility that significant AI-driven change may be implemented inconsistently, with inadequate stakeholder engagement, training, and adoption support.

Proposed Action Plans:

Areas highlighted within this issue will be actively discussed by leadership and necessary steps will be taken to ensure AI is well understood and appropriately rolled out within the organization. Further discussion and direction required for a mindset change (experimentation mindset vs. mindset of failure) will be looked into and appropriately socialized considering all other aspects impacting the organization.

Responsible Person:

ELT and P&C Division with Support from all other Divisions – March 31, 2027

4. Continued Focus on AI Supporting Pillars – Data, System Architecture, Information Security and Performance Measurement

In an era where AI drives innovation across industries, data integrity, resilience, security and responsibility are no longer optional, they are the fundamental pillars of AI. Achieving this requires robust data architectures, cyber-resilient designs, and continuous monitoring to ensure consistent performance, while embedding responsibility into every layer of the organization.

Observations:

A. Data Quality and System Architecture

BCLC has made notable progress in strengthening its data governance. The creation of a formal Enterprise Data Strategy and Enterprise Data Office (EDO) is critical for successful AI adoption. Progress has accelerated since earlier this year, particularly in monitoring player health data and integrating it into new systems.

The current data and analytics program is scheduled to complete by FY27, creating a natural opportunity to layer AI strategy over a robust data foundation. On review, Audit Services noted a few challenges that BCLC needs to address:

a. Not all data sources have been migrated to the future-state architecture or aligned with the data governance framework. Centralized definitions for key data elements are actively evolving as part of the broader data governance initiatives. Continued focus is required to support enterprise-wide AI enablement.

b. Data is not significantly leveraged in automated ways or is AI-driven. For example, opportunities exist in identifying behavioral patterns, triggering personalized experiences, and optimizing casino layouts through predictive insights.

c. Legacy systems with decentralized logic persist, creating challenges and constrianing AI scalability.

d. Data needs have evolved from siloed business-unit analysis to enterprise-wide insights. However, systems often do not align, partly due to limitations caused by technical debt.

Integrated quality data is essential for AI. Each bad record can confuse the model and lead it to provide incorrect answers.

e. The organization does not fully understand how data is used or shared through AI tools. Example, a unified view across online, in-person, loyalty, and marketing channels is essential for accurate and ethical AI use (Absence of a 360-Degree Player View).

Top Seven Risks from MIT AI Risk Repository Related to Data Quality and Architecture	
1	Poor data quality (inaccurate, incomplete data)
2	Architecture scalability issue (performance bottlenecks)
3	Security & Privacy (breaches, personal information exposure)
4	Poor metadata and linkage tracking (no traceability)
5	Inadequate data governance (lack of policies, unclear ownership)
6	Data silos & fragmentation (isolated systems, poor integration)
7	Lack of standardization (inconsistent formats)

B. s. 15(1)(l)

AI can predict threats, but only strong security controls can prevent them.

C. Success Metrics and ROI

AI performance metrics should encompass a broad range of AI capabilities, including generative AI, machine learning models, and predictive analytics, to ensure value realization and risk management across all AI-driven initiatives. Establishing measures and tracking them builds trust, improves decision-making and strengthens overall management.

a. Currently, AI initiatives operate without a formal framework to define success criteria or measure ROI.
b. BCLC does not have defined Key Performance Indicators (KPIs) to monitor AI model performance, impact, and risk. Metrics for accuracy, fairness, and operational reliability are absent.
c. AI initiatives are often approached as a new implementation rather than being integrated into broader project delivery.

What gets measured gets managed: Define KPIs for accuracy, fairness, and reliability.

Examples of AI Metrics to Measure Value	
1	KPIs for evaluating AI performance
2	Tracking changes in productivity
3	Evaluate generative AI investments
4	Track non-financial benefits
5	Value creation from generative AI investments

In conclusion, metrics such as these should be tracked, recorded, and reported to C-Suite periodically for information and key decision-making. With the pace at which AI is evolving within the corporate ecosystem, it is essential leaders are well informed and are on top to take calculated risks and make critical decisions for long-term success of the organization.

IMPACT:

Data and information security are extremely important and crucial for the reliability and accuracy of decisions made by AI systems. The above highlighted challenges can increase the risk of poor business decisions, security incidents and undermine trust in AI outcomes and BCLC's ability to use AI technology safely and effectively.

Without KPIs, AI performance issues and compliance risks may go unnoticed, undermining transparency and stakeholder trust. Without structured knowledge sharing, insights remain siloed, limiting strategic reuse, slowing innovation, and weakening AI culture and ROI.

PROPOSED ACTION PLANS:

Leadership will look into all aspects highlighted – data quality, system architecture, security and performance measures and consider upgrades, changes, and incorporation of new practices to strengthen the overall AI framework that is being rolled out within the organization.

RESPONSIBLE PERSON:

BT and SP&EI Divisions with Support from all other Divisions – March 31, 2027

5. Further Focus on Vendor and Third-Party Management in Relation to AI

Effective vendor management is critical for mitigating third-party AI risks. The organization must conduct due diligence to ensure vendors align with the organization's ethical AI principles and operational standards. Contracts should clearly define roles, data governance and accountability for model performance and fairness. Ongoing monitoring is essential to verify continued compliance throughout the AI system lifecycle.

Observations:

A. Third-Party Reliance on AI Powered Solutions

a. BCLC relies heavily on vendor-provided AI solutions to support key operations. However, there is limited transparency into the underlying models and decision-making logic used by these third-party system. For example, certain vendors are developing AI models for various divisions of the organization, yet there are insufficient insights into how algorithms work or decisions are derived.

b. Vendor assurances alone are insufficient, BCLC must develop internal technical expertise and implement a structured process to evaluate and monitor vendor AI outputs effectively. The lack of insight could impact BCLC's ability to assess risks, ensure compliance, and maintain accountability for AI-driven outcomes.

B. Vendor Contracts to be Abreast to Evolving AI Landscape

a. Vendor contracts need to evolve to keep pace with evolving AI landscape. Aspects like underlying algorithms and the corresponding calculations which result in the AI output should be part of the information vendors need to provide. This will ensure BCLC is able to understand and ensure there are no biases or compliance concerns impacting organizational trust and integrity.

AI capabilities are increasingly embedded in vendor solutions, but transparency on model design, data sources, and fairness assessments remains limited.

C. Vendor Alignment Opportunities

BCLC's engagement with third party vendors has provided valuable insights into how AI partnerships can be further strengthened moving forward. The arrangement although working well, has surfaced certain areas for improvement to build a more consistent and scalable approach to vendor oversight. One that balances structure with the flexibility needed in a fast-changing AI landscape. Areas to focus include:

a. Define Onwership and Accountability – Clearly assign roles and responsibilities for vendor-managed products and services to avoid ambiguity.

b. Develop a Standardized AI Vendor Framework – Create a flexible but consistent framework that outlines expectations for governance, data security, and performance management across all AI vendors.

c. Implement Governance and Reporting Protocols – Ensure steering committee decisions, vendor roadmaps, and performance updates are documented and communicated regularly.

d. Establish a Consistent Vendor Intake and Evaluation Process – Define criteria and workflowss for assessing new AI use cases, including risk, value, and alignment with strategic priorities.

e. Clarify Data and Security Requirements – Include data residency, privacy, and control expectations in vendor contracts and onboarding materials.

Through these steps, the organization can both strengthen its engagement with vendors providing AI solutions and establish a repeatable model for future AI partnerships. One that supports innovation, safeguards data, and confirms performance, all while remaining adaptable to the evolving AI landscape.

IMPACT:

Lack of transparency in AI initiatives can lead to compliance risks, operational disruptions, and diminished stakeholder trust. Weak vendor contracts and inconsistent management frameworks further increase the risk of service failures, data security issues, and reputational harm. Establishing clear roles, responsibility and accountability is essential to scale AI responsibly and realize its strategic value.

PROPOSED ACTION PLANS:

Transparency on AI initiatives will be covered through management response to recommendation #2 above. Procurement will establish a framework, process, and approach, with Legal, Architecture and AI Steering to address AI focused procurements.

RESPONSIBLE PERSON:

FCS Division and other stakeholders as required – March 31, 2027

Distribution List

Sandy Austin
Dan Beebe
Pat Davis
Gary Foster
Jeremy Hopwood
Alan Kerr
Martin Lampman
Mark Lane
Marie-Noëlle Savoie
Sarah Turtle

Communications

Laura Piva-Babcock

Our Audit Team

Donna Dickson
Dushan Koralage
Jug Lalli
Cecilia Vargas Herring
Rao Wandawasi
Karen Wang