Financial Services Regulatory Commission
Antigua and Barbuda
Division of Gaming

Sound Practices for the Management of Operational Risk for Interactive Gaming & Interactive Wagering Companies

November 2005

Sound Practices for the Management of
Operational Risk for Interactive Gaming & Interactive Wagering Corporations

Authority

1.1 Section 316 (4) of the International Business Corporations Act (IBC Act) requires the Commission to take any necessary action required to ensure the integrity of the International Business Corporation sector. The International Business Corporations (Prudential Management of Licensed Corporations) Regulations, 2004 - Statutory Instrument No. 9 of 2004- prescribe that a licensed corporation:

- shall carry out its business in a prudent manner in accordance with the industry standards and best practices and any guidelines or directions issued by the Commission [regulation 4].
- establish and implement policies, practices and procedures relating to identification, measurement, monitoring and control of *default risk, liquidity risk, legal risks and operational risks [regulation 8(1) (g)] and the Interactive Gaming and Interactive Wagering Regulations 87 to 94.*
- shall be guided by such guidelines or directions as the Commission may issue in relation to policies, practices and procedures of a licensed corporation [regulation 6].

1.2 These guidelines are being issued for the guidance and compliance by the corporations licensed to carry on *interactive gaming and interactive wagering business* but shall be applicable to other licensed corporations also to the extent they are relevant.

2 Background

2.1 'Operational risk' is 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'. The definition includes legal risk but excludes strategic and reputational risk. Operational risk is a distinct class of risk similar to default and market risk. Examples of operational risk include:

- Internal and external fraud
- Employment practices and workplace safety
- Clients, software, games and business practices
- Damage to physical assets
- Business disruption and system failures (telecommunications, gaming software and betting and wager errors)
- Execution, delivery and process management (for example, data entry errors, collateral, unapproved access given to player accounts, and vendor disputes.)

2.2 Operational risk differs from other IGIWC risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity. At the same time, failure to properly manage operational risk can result in a misstatement of a company's risk profile and expose the company to significant losses.

2.3 Management of operational risk includes identification, assessment, monitoring and control/mitigation of risk.

3 Developing an Appropriate Risk Management Environment

3.1 The board of directors should be aware of the major aspects of the IGIWC operational risks as a distinct risk category that should be managed, and it should approve and periodically review the IGIWC operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/ mitigated.

3.2 The board should provide senior management with clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by senior management.

3.3 The framework should cover the company's appetite and tolerance for operational risk, as specified through the policies for managing this risk and the IGIWC prioritization of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the company. It should also include policies outlining the IGIWC approach to identifying, assessing, monitoring and controlling/mitigating the risk. The degree of formality and sophistication of the IGIWC operational risk management framework should be commensurate with the company's (private or publicly listed) risk profile.

3.4 The board should establish a management structure capable of implementing the IGIWC operational risk management framework. It should establish clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest.

3.5 The board should review the framework regularly to ensure that the IGIWC is managing its operational risks and conforms to industry best practice. If necessary, the board should revise its operational risks so that all material operational risks are captured.

4 Internal Audit

4.1 The board of directors should ensure that the IGIWC operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

4.2 The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit program is appropriate to the risk exposures. Audit should periodically validate that the IGIWC's operational risk management framework is being implemented effectively across the IGIWC.

4.3 Where audit function at some IGIWC's (particularly smaller companies) has initial responsibility for developing an operational risk management program, IGIWC's should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner.

5 Senior Management

5.1 Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole on-line gaming organization, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the on-line gaming company's material products, activities, processes and systems.

5.2 Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and ensure that the necessary resources are available to manage operational risk effectively. Senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.

5.3 Senior management should ensure that on- line gaming company's activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, that staff responsible for monitoring and enforcing compliance with the IGIWC risk policy have authority independent from the units they oversee and that the on-line gaming company's operational risk management policy has been clearly communicated to staff at all levels in units that incur material operational risks.

5.4 Senior management should ensure that staff responsible for managing operational risk communicates effectively with staff responsible for managing credit, market, and other risks, as well as with those in the company who are responsible for the procurement of external services such as gaming software provider, alternate payment solutions and outsourcing agreements (customer service support and affiliates and associates).

5.5 Senior management should also ensure that the on-line gaming company's remuneration policies are consistent with its appetite for risk. Remuneration policies which reward staff that deviate from policies (e.g. by exceeding established limits) weaken the company's risk management processes. Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transactions volumes, in particular, should be well documented and disseminated to all relevant personnel.

6 Identification, Assessment, Monitoring and Mitigation/Control of Operational Risk

Identification

6.1 On-line Gaming companies should identify and assess the operational risk inherent in all proprietary software and games, activities, processes and systems. Effective risk identification considers both internal factors (such as the on-line gaming company's structure, the nature of the company's activities, the quality of the company's human resources, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the gaming company's objectives.

Assessment

6.2 On-line Gaming company's should ensure that before new games, software activities, processes and systems are introduced or undertaken, the operational risk inherent in them is adequately assessed.

Monitoring

6.3 On-line Gaming company's should implement a process to regularly monitor operational risk profiles and material exposures to losses. In addition to monitoring operational loss events, on-line gaming companies should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new games and/or software, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable the on-line gaming company to act upon these risks appropriately.

6.4 There should be regular reporting of pertinent information to senior management and the board of directors. The board of directors should receive sufficient higher-level information to enable them to understand the gaming company's overall operational risk profile and focus on the material and strategic implications for the business.

Mitigation/Control

6.5 On-line Gaming company's should have policies, processes and procedures to control and/or mitigate material operational risks. For all identified risks the company should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the on-line gaming company should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

6.6 Some important constituents of a mitigation/control program are:

- Formal, written policies and procedures
- Strong control culture that promotes sound risk management practices
- Appropriate segregation of duties
- Assignment of responsibilities such that there is no conflict of interest.
- Close monitoring of adherence to assigned risk limits or thresholds
- Maintaining safeguards for access to, and use of, assets and records
- Ensuring that staff have appropriate expertise and training;
- Identifying business lines or gaming/wagering returns appear to be out of line with reasonable expectations (industry bench marks with respect to percentages) (e.g., where a supposedly low risk, low margin gaming activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach);
- Regular verification and reconciliation of transactions and accounts; and.
- Investments in appropriate software technology and information technology security (However, on-line gaming companies should be aware that increased automation could transform high-frequency, low-severity losses into low frequency, high-severity losses.)

7 Outsourcing

7.1 On-line gaming company's should establish policies for managing the risks associated with outsourcing activities. An on-line gaming company's use of third parties does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws.

7.2 Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers (software providers and customer service support) and the outsourcing company. Furthermore, IGIWC need to manage residual risks associated with outsourcing arrangements, including disruption of services.

7.3 Potential impact on operations and customers due to any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties should be identified. The board and management should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the on-line gaming company for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment.

7.4 On-line Gaming company's should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the internet gaming industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the on-line gaming company may need to consider contingency plans.

7.5 On-line Gaming company's should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

8 Contingency Plans

8.1 On-line Gaming company's should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. Such plans should be in place for all critical business processes and take into account different types of plausible scenarios. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption.

8.2 On-line Gaming company's should periodically review their disaster recovery and business continuity plans so that they are consistent with the on-line gaming company's current operations and business strategies. These plans should be tested periodically to ensure that the company would be able to execute the plans in the unlikely event of a severe business disruption.

9 Disclosure

9.1 On-line Gaming company's should make sufficient public disclosure to allow market participants to assess their approach to operational risk management. The amount of disclosure should be commensurate with the size, risk profile and complexity of an on-line gaming company's operations and should be in a manner that will allow players, investors and counterparties to determine whether a on-line gaming company effectively identifies, assesses, monitors and controls/mitigates operational risk.

10 Review by the Commission

10.1 The on-line gaming company's policies, procedures and practices related to operational risks would be subject to review by the Commission as part the examination conducted under the IBC Act and the Interactive Gaming & Interactive Wagering Regulations (IGIWR).