Intellect Design Arena Ltd

Risk Management Policy

Adopted by the Board of Directors on July 28, 2021

TABLE OF CONTENTS

Introduction

Intellect Design Arena Ltd. (The Company) is committed to transparency, integrity and accountability in all its affairs towards its clients, shareholders, associates, distribution partners and regulators. The Company is determined to expand business exponentially, provide high quality designs & innovative solutions for its clients and maximize returns for the Company's shareholders. The organisation believes in the fundamental economic principle of "higher the risk - higher is the reward" and therefore with increase in the size, scale and complexities of the business, it is imperative for the Company to take calculated risks to achieve objectives of superior earnings & profitability. Thus, it is important for the Company to have in place a robust, organized and effective Enterprise risk management systems, processes & technologies. Therefore, the Company have established the Risk Management Policy ("Policy") which will allow to build & maintain its core expertise around understanding and managing enterprise wide risks more effectively and efficiently.

The Policy takes into consideration the regulatory requirements in accordance with the IT Act, 2000, Companies Act, 2013 ,SEBI(Listing Obligations and Disclosure Requirements) Regulations, 2015 local as well as other applicable laws and regulations.

1.1 Definition

Risk management is the process of identification, measurement and mitigation of risks in order to minimize their impact to the business / organisation.

1.2 Objective:

The objectives of the Risk Management Policy are to:

1. formulate and communicate a consistent approach to manage the Enterprise wide risks,
2. provide guidance to establish the standards tools & procedures on managing various types of risks,
3. outline the Risk Management agenda of the Board of Directors and set forth the roles and responsibilities of the various internal & Board committees established to manage the risk agenda of the Company.
4. establish a common risk language through the risk framework (including ESG related risks) consisting of standard risk categories, consistent risk identification, issue rating guidelines, scoring and prioritization methodologies and a centralised risk recording mechanisms.

1.3 Policy Scope:

The Policy applies to all the functions, departments and types of risks – internal and external in nature to which the Company is exposed.

2.1 Risk Management Principles

The Risk Management Policy of the Company is established not to eliminate the risk and volatility, but to understand and effectively manage the risks faced by the company through:-

1. identification of the Company wide risks existing & potential risks,
2. review of the design & operating effectiveness of the internal controls and residual risk exposures of the business & operational process / procedures,
3. assessment of the likelihood and impact of the risks through proper quantification,
4. evaluation of the risks vis a vis tolerances or thresholds of the Company;
5. providing recommendations & facilitating corrective measures or mitigation strategies to minimize the risk impact ;
6. assessment of the Company's financial resources to manage the business given its risk tolerance and business plan.
7. timely reporting and review of risks by the stakeholders / management to enable decide on the mitigation strategy.

2.2 Three layers of defence:

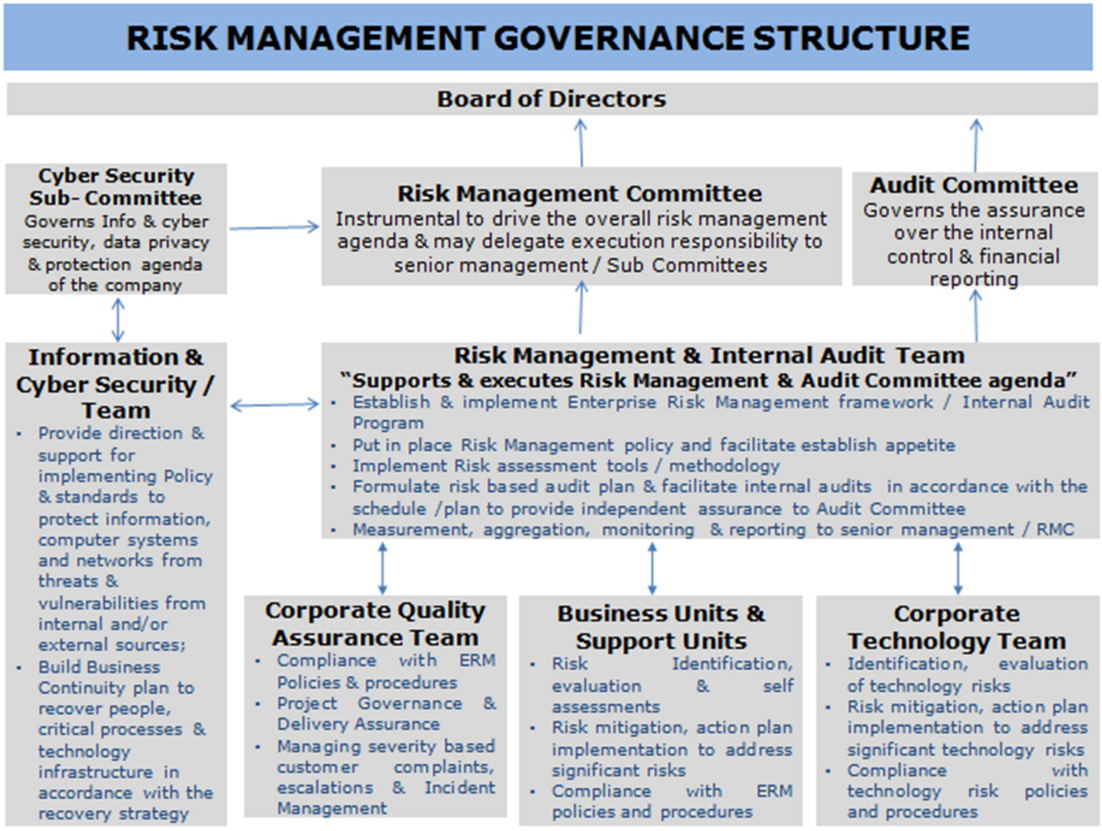
2.2.a.1 **First line of defence:** It is the primary responsibility of the business & process owners to design & operate the strategy, performance management and effective risk control mechanisms in its day to day functioning. Said to be 1st line - as controls are designed into systems and processes along with adequate managerial & supervisory checks to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events **[Functions Own and manage their risks – Functional Management]**

2.2.a.2 **Second Line of defence:** Facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owner in defining the risk exposures and reporting adequate risk information throughout the organization. This is an oversight of the risk framework by the risk management committee, Chief Risk Officer, and the risk management functionaries working with their counterparts in the functional areas.**[Function that provides/conduct Oversight & Internal Monitoring of Risks – Risk Management, Compliance and other Control/Assurance functions]**

2.2.a.3 **Third line of defence:** This involves a internal audit that ensures the independence and effectiveness of the Company's systems & processes. [**Function that provide independent assurance – Internal Audit]**

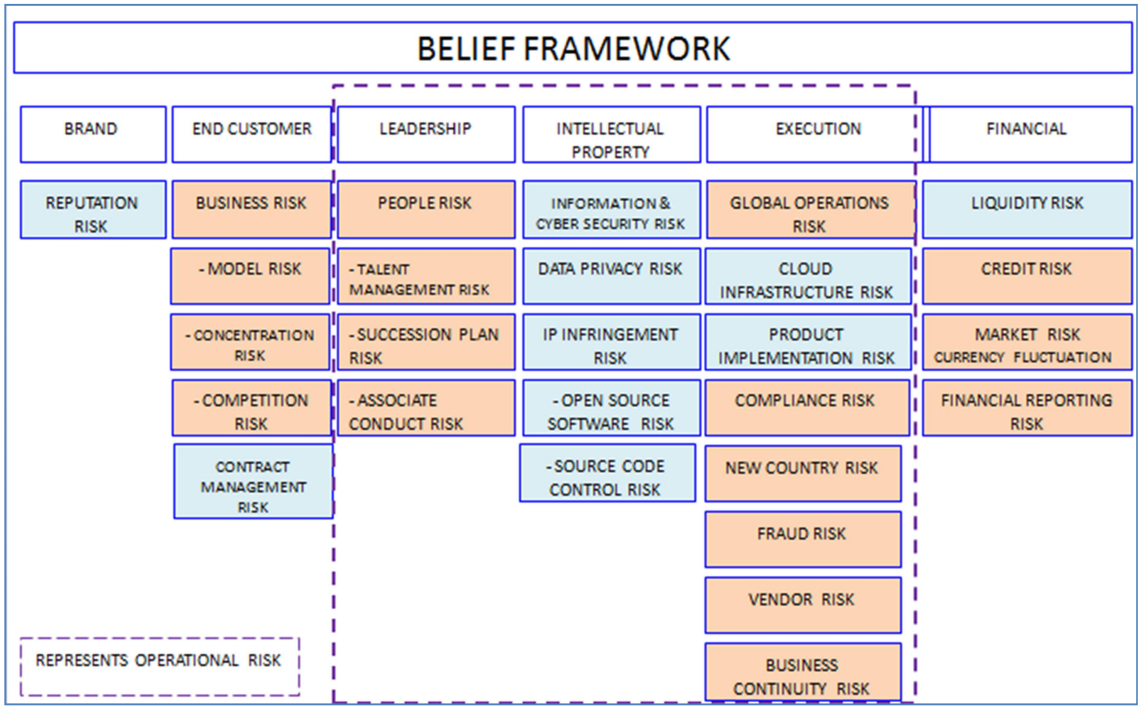
2.3 Risk Governance Structure:

The Board of Directors shall establish appropriate systems to regulate the risk appetite & risk profile of the Company. In order to develop the strong risk management system & mitigation strategies and ensure coverage of wide spectrum of risks to which the Company is exposed to, Company's Board of Directors have established following Governance structure:



2.4 Risk Framework - Classification and Definition

Risks within the Company are classified under BELIEF ((Brand, End Customer, Leadership, Intellectual Property, Execution & Finance) framework as follows:



Below are the risk definitions of few of the major risk categories:

BRAND

a) **Brand / Reputational Risk**: This is the risk of loss arising on account of negative publicity, company's business practices, customer complaints or litigations or may heighten in case of subdued financial performance / negative investors perception or sentiments / Unmeasured Press statements / Product related issues / Delivery Failures / Customer relationships / Client escalations / Inter - Clients feedbacks / Associates misbehaviours / Commercial disputes / Legal violations etc. Risk severity accentuates due to increased use of social media, mobile & other internet based applications in today's corporate world.

END CUSTOMER

b) **Business Risk**: This is the risk of inability to earn adequate profits or incur losses on account of existing business uncertainties such as failure to meet the business plans and unforeseen events in the future such as change in consumer preferences, increase in the market competition, business

concentration or obsolescence of the products & services resulting in the business failure.

Contract Management Risk: It is the risk arising from non performance of contractual obligations and may accentuate in case contract formulations are not commensurate to the organisations risk appetite, commitments, delivery capabilities and customer expectations.

LEADERSHIP

c) **People Risk**: This risk is associated with the talent management, succession planning & associate conduct within and outside the organisation.
   i. **Succession Plan**: Succession plan for key / critical manpower if not adequate may exert strain on company resources in case of unplanned attrition.
   ii. **Talent Management**: Risks pertaining to the ability to attract or retain top or key talent with specialised skill sets for the organisation.
   iii. **Associate Conduct**: Risks arising on account of inappropriate conduct such as Frauds, sexual harassment, criminal attempts, bribery, breaches in code of conduct, professional negligence ; errors & omissions or violation of Company policies such as code of conduct, conditions of employment ; Insider trading etc. and may jeopardise work culture / reputation / asset / property damage or business performance

INTELLECTUAL PROPERTY

d) **Information & Cyber Security Risk:** It is the risk arising from the Internal & external cyber threats which if not appropriately managed can potentially result in compromise of the system leading to system failures, downtime, data leakage, change in system behaviour etc. and may significantly disrupt core business operations & has the potential to damage Company's Brand Image / reputation**.**

e) **Data Privacy & Protection Risk:** It is the risk arising from inadequate or inconsistent controls to handle the PII data of the customers / associates that are subject to data privacy laws of various states. Risk accentuates on account of cloud hosting, widespread usage of emerging technologies and business models around data as a core element.

f) **IP Infringement Risk**: It is the risk that may arise out of Infringement of copyrights licenses, patents, trademarks,, technologies, or business processes as IP users or IP providers on a/c of inadequate licenses, extensive use of open source codes / tools without abiding to their T&Cs, mis-use of Company's IP by the service providers or tampering of intellect IPs resulting in a negative impact on the business (fines / penalties or reputational damage)

EXECUTION

g) **Operational Risk**: This is the risk of loss arising on account of failure in the process, people, systems of the company or from the external events as illustrated below:

i. Fraud (Internal / External)
ii. Employment practices
iii. Client & business practices
iv. Product implementations
v. Damage / loss of physical assets
vi. Business disruptions & system failures
vii. Execution, delivery & process management
viii. Legal & regulatory compliances

h) **Cloud Infrastructure Risk:** It is risk that may arise on account of non compliance to SLAs or unique contractual agreements with the cloud service providers or customers, non deployment of adequate security measures or security breaches, lack of availability of highly skilled resources to manage cloud environments or non compliance to the heightened regulations like GDPR which may result in financial implications (imposition of fines & penalties) or reputation damage.

i) **Product Implementation Risk:** Risks arising on account of delays, errors or omissions in implementations & support could hamper delivery capabilities leading to multiple risks such as delayed implementations, collections, violation of contractual commitments, fines / penalties and damage to the Brand image.

j) **Fraud Risk:** Risk arising on account of inability to prevent, detect, measure, monitor & report the potential collusion touch points , fraud events or criminal hackings which may result in revenue leakage , financial losses or the reputation damage for the Company.

k) **New Country Risk:** Risks arising on account of failure to effectively study, evaluate, identify, analyze & address the country specific risks at the time of entry into a particular geography may adversely affect long term interests of the organisation

l) **Business Continuity Risk**: This is the risk of unplanned interruptions in the business on account of an accident, disaster, emergency or threat.

m) **Legal, Compliance & Regulatory Risk**: Legal Risk is the risk of loss from legal actions, disputes against the Company arising from the failure to adhere to the contractual agreement.

Compliance & Regulatory risk is the risk that a change in laws and regulations and its non adherence may materially impact the Company or the industry or its client segment.

FINANCE

n) **Liquidity Risk**: This is the risk of loss arising on account of non-availability of cash / cash equivalent or mismatch of cash flows to meet the company's liabilities & claims as and when they arise.

o) **Market Risk**: This is the risk of loss arising out of fluctuations in the value of its assets, liabilities or the income from its assets. These fluctuations could be on account of changes in the Interest Rates; Currency values; Equity / Commodities and macro-economic factors like Gross Domestic Product, Inflation & Gross Capital formation.

p) **Credit Risk**: This is the risk of loss of principal or financial rewards arising from counterparty's failure to repay the loan or meet a contractual obligation. Credit risk arises whenever Company is reliant on future cash flows to pay a current debt. It includes Off-balance sheet risks and proprietary risk.

q) **Financial Reporting Risk**: Risks arising on account of key Internal controls over financial reporting if not designed, identified & operate effectively may result in mis-statements going unnoticed and impact the true & fair view of the financial / operational results of the Company.

2.5 Interaction with business / operations teams

The Risk management team shall periodically interact with the Business and Operations team as part of their role. The focus of these interactions shall be as follows:-

a. Assessment of current risks, their mitigation and identification of emerging risks
b. Review of the key internal policies and processes governing operations / roles of these departments and inputs of risk on the same
c. Review of key strategic / operating decisions taken or proposed, identifying associated risks & mitigation measure and their impact on solvency and profitability position of the company along with other relevant stakeholders as per the defined standard operating procedure
d. Identification of key risks for the department / function, development / modification of key risk indications and defining appropriate tolerance levels / Risk Appetite.
e. Creating awareness on Risk Management and the role of the first line of defence (Business / Operations)

2.6 Risk Management Approach

Risk Management approach consists of 5 major steps:

a) **Risk identification:** Identifying the risks is the fundamental step towards effective risk management. The Company regularly assess the environment (internal / external) in which it operates and identify what can go wrong & therefore cause a financial, customer or legal / regulatory impact to the company. Tools to be used for the same include :-

i. Periodic RCSA evaluation
ii. Key strategic changes in the business / operations
iii. Key industry changes
iv. Key regulatory changes
v. Internal / external frauds
vi. Loss data analysis
vii. Outsourcing of activities

b) Risk evaluation: The Company evaluates its risk severity based upon 2 factors: i) understanding the likelihood of risk occurrence in the light of current size, scale & complexity of the business and the external environment in which it operates; and ii) impact of the risk occurrence. Thus, severity is broadly classified as High, Medium or Low based on the likelihood of its occurrence and its impact to the Company. Refer to the Company's Issue Risk rating guidelines for detailed information on evaluating risk severity.

c) Risk prioritisation: The Company prioritizes risks basis it's Risk Appetite. It is the level of risk exposure that a company is ready to live with it or tolerate / accept. Every function defines its thresholds or tolerance levels to enable undertake well calculated risks & facilitate effective decision making process in light of threats & opportunities. Risk management department facilitates that the risk owners to articulate risk appetite for measuring the current risk exposures against the set tolerances and monitors them in order to determine the risks which require mitigation and or management review.

d) Risk mitigation: Based on the severity of the identified risk, management evaluates risks with its risk appetite or tolerance limits set and develops an appropriate action plans to mitigate or minimize the impact of the risks which are outside of the defined threshold.

e) Risk monitoring & review: The Company regularly monitors and report the risks and their mitigation plans to the senior management & Board Committees

to enable them understand overall risk exposure which company face and well equip them to take the appropriate measures. The risk monitoring framework shall comprise of the following:-

- Key Risk Indicators
- RCSA testing results
- Solvency position and stress testing results
- Vendor / Partnership performance evaluation results
- BCP testing results

2.6 Defining the risk appetite / thresholds

Risk Appetite refers to the nature & extent to which the Company is willing to take, accept or tolerate significant risks in achieving its stated objectives. The Company's tolerance levels differ across various products, processes and systems and enable in managing its risk effectively.

The following approach is recommended for defining the risk appetite of the company:-

1. Post setting of business strategy / budgets for the year, the Risk Management Committee shall define the risk appetite for the next financial year and set the risk appetite limits for various quantitative (Profitability, Solvency, Liquidity, etc.,) and qualitative (Reputation, Market Position, etc.,) parameters.

2. Based on the defined risk appetite, tolerance limits for the KRIs are defined within the overall threshold. These shall be presented to the internal committee & thereafter to the RMC of the Board for the review and approval.

3. The defined risk appetite and KRI, tolerance limits shall be monitored by the Risk Management Department & presented to the RMCB on a regular basis.

   Also, in case a strategic decision is proposed by the company, the same shall be reviewed and by the internal working committee and its impact on the financials shall be analysed & accordingly Risk Appetite level be defined and communicated to the Risk Management Committee for review & approval. Based on the inputs of the internal committee and / or Risk Management Committee of the Board, the risk appetite levels may be reset and any breaches of tolerances shall be approved.

The factors considered while defining the right level of tolerances/ thresholds for

the Company are:

a. different risks associated to the products, processes and systems;
b. capital required to effectively manage these risks;

propensity to undertake given level of risk and to exercise the control around the products, processes & systems; and

c. assessment of the extent of risk which can be retained in the company's books and therefore require to transfer some of the risks through re-insurance;

2.7 Risk Management Tools / Methodology:

A Risk Management Plan is prepared and presented to the RMC of Board on an annual basis. The plan contain the following details:-

- Proposed department / function wise RCSA testing plan
- Current KRIs, their tolerance levels and the enhancements proposed
- Risk Assessment outcomes

2.7.1 Capital Assessment for future uncertain events: The Company forecasts its future capital requirements through business planning exercise. The sensitivity analysis is performed on the Company financials to determine the capital requirements based on future uncertain events such as

- Business volumes changes;
- Change in product mix;
- Currency Fluctuations.
- Cost variations
- Productivity changes.
- Business mix change

This facilitates the Company to define its growth objectives & tolerances given the planned levels of shareholder capital.

The solvency / cashflow position of the company is periodically reviewed and the presented to the Audit Committee meeting.

2.7.2 Profitability Analysis: The Company shall conduct periodic analysis of the product profitability and evaluates the risk factors impacting downfall and plan the mitigation strategies to align the margins to the Company's growth objectives. It may use Internal Rate of Return, New Business Margin , Profit Margin or any other measure deemed relevant from time to time or as required by regulations.

Impact of various strategic decisions on the profitability of the company shall be reviewed and presented to the RMCB periodically.

2.7.3 Control Self-assessment: Self-assessment of the control environment is the effective mechanism for the risk identification across the company and performed by the respective departments with the objective is to identify & document the gross risks, control mitigants, monitoring mechanisms, residual risk exposures not fully mitigated and the required action plans through Risk Assessment Matrix / templates.

The CSA shall be conducted on annual basis and RMCB shall be updated on the status of CSA and movement in the risks profile of the functions / departments.

2.7.4 Risk Assessments / Reviews: Deep dive reviews shall be performed for select functions / processes in accordance with the agreed Risk Management Plan and residual risk exposures are tabled and discussed with the management. A Risk management plan shall be prepared on an annual basis and presented to the RMC for approval. The activities shall be carried out basis the approved plan and the results shall be presented to RMC. **Refer to Information & Cyber Security 2.7.11 for CSG risk assessments.**

2.7.5 Enterprise Key Risk Indicators: Basis identified risk exposures, the company defines the key risk indicators at enterprise level and also for the specific functions reviewed / assessed to monitor the residual risks on ongoing basis.

- Key Risk Indicators are rated as Red, Amber or Green based on the tolerance levels set by stakeholders & approved by the RMC;
- Moreover, Risk Heat Map is developed for specific functions which have a risk evaluation checklist providing detailed guidelines on each risk parameter to facilitate objective assessment of those risks.

The KRIs shall be reviewed and enhanced from time to time and the tolerance limits for the same shall be reviewed. Impact of any strategic business decisions on the same and the past KRI level shall be reviewed to set the tolerance limits. KRI monitoring shall be an on-going process and status of the same shall be presented to the RMC.

2.7.6 Customer Complaints redressal: The Company shall have in place proper procedures & effective mechanisms to address complaints / grievances of efficiently and speedily. The procedures shall consider the roles, responsibilities, escalations and actions for handling of the receipt and closure of the Grievances along with the service level agreements.

2.7.7 Vendor Risk Management: The Company shall have established the process for vendor due diligence prior to its onboarding & registration. Information Security requirements shall be considered at all stages throughout vendors having access / handling the Company's system/data. The risks to the Company's information & related processing facilities from business process

involving external parties shall be identified and appropriate controls shall be implemented prior to the engagement, during engagement & at the time of termination or renewal of the engagement.

2.7.8 Compliance: The Compliance function of the Company shall work with the business management to establish, implement and maintain compliance policies and procedures facilitating the functions to comply with new & applicable regulations & internal standards including but not limited to Anti Money Laundering, Anti Bribery guidelines etc. Associates are imparted trainings to built the compliance understanding. The Company shall also provide guidance & suggest remedial measures to business management for adherence to the compliance requirements. The Company shall coordinate with the regulators – SEBI / Company Law Board etc. in response to their queries / audit etc. and has built the mechanisms to track all the regulatory filings and correspondences.

Compliance with the regulatory and internal guidelines of the company shall be reviewed by the internal auditors on an on-going basis and the same shall be part of their scope. The scope on compliance shall be drafted / signed off by the Compliance department of the company.

2.7.9 Sales Compliance: The Company shall establish monitoring process to encourage right sales, delivery & implementation practices, promote ethical sales behaviour so that clients are treated fairly and thereby minimize the risks around practices of mis-selling. This shall be achieved through regular business review meetings, quality reviews, self assessments and compliances.

2.7.10 Project Implementation / Delivery Excellence Framework: The Company shall follow the Delivery Excellence framework wherein project team shall identify and assess risks at the beginning of the project and on a continuous basis during the course of the project. Project Manager shall analyze and prioritize risks based on impact and probability of occurrence and identify suitable mitigation measures or contingency plan. Based on project dynamics, Project Manager shall also monitor and periodically revise and reassess the impact and probability and refine risk implementation strategy. As part of compliance checks, LOB Quality team shall review the implementation risks along with the mitigation/contingency plans.

2.7.11 Fraud Control: The Company shall deploy mechanisms to perform the investigation of suspected fraudulent activities, monitoring the fraud indicators and trends. Also, various offsite activities and analytics shall be undertaken to identify the potential red flags and strengthen the process controls to mitigate fraud instances. Various campaigns around fraud prevention are run to increase the overall awareness and responsiveness towards fraud. The fraud instances are reported to senior management, Risk Management Committee.

2.7.12 Information & Cyber Security: The Company shall have well defined Information & Cyber Security policy to :

a. Provide direction and support for information & cyber security;
b. Facilitate to establish the governance framework on Information Security Management System (ISMS) Standards and Procedures to protect the Company's information assets;
c. Provide guidance for standards to protect information, computer systems and networks from threats and vulnerabilities from internal and/or external sources;
d. Achieve compliance with legislative, statutory, regulatory, legal and contractual requirements;

The Company shall have a risk management program to undertake information security risk assessment for target environments (e.g. critical business environments, business processes, business applications, computer systems and networks) on an annual basis. There shall be formal, documented standard/procedures for performing information risk assessments, results of which shall be reported to business owners / senior management. The risk management programme shall be integrated with wider risk management activities and execute monitoring procedures & other controls to detect errors, identify breaches, plan mitigation to facilitate effective implementation of remedial measures. Refer to the Information Security Policy ; Risk & Incident Management Policy.

2.7.13 Business Continuity Planning: The Company is committed to provide uninterrupted services to its customer and shall build a Business Continuity plan to recover its people, critical processes & technology infrastructure in accordance with the defined recovery strategy.

The company has a defined BCP policy in place which shall be periodically reviewed by the Risk Management Committee. BCP testing shall also be carried out for all the activities / functions of the company *(both internal & outsourced)*. Annually, a BCP plan shall be prepared and presented to the Risk Management Committee for approval. The BCP team shall conduct testing as per the plan covering various offices / branches of the company. Status of BCP tests and results shall be periodically placed before the Risk Management Committee.

2.7.13 Insurance: The company shall appoint Risk & Insurance advisory to advice on the risk and insurance coverage. The following Insurance coverage shall be taken to mitigate risks.

i. Errors & Omissions Insurance – To safeguard against any loss arising of an error, negligent act or omission which would result in failure in performing the professional services or duties for others.
ii. Cyber Liability Insurance - To safeguard against any loss arising out of a

security breach and or privacy breach that would result in sensitive or unauthorized data or information being lost or compromised.

iii. Crime Insurance - To safeguard against any direct financial loss of property, money or securities arising out the fraudulent activities committed by the employee or in collusion with others.

iv. Directors & Officers Liability Insurance - To safeguard against any loss arising out of a wrongful act made by the Directors, Officers and Employees of the organization with reference to the company's business operations and activities.

v. Commercial General Liability Insurance - To safeguard against Third Party bodily injury or property damage arising out of our business operations.

vi. Standard Fire & Special Perils Insurance - To protect the company's Assets (movable & immovable Assets) from the risk of Fire or Perils.

2.7.14 Risk Awareness – One of the measures to manage the risks within an organization is to create awareness of the risks amongst the employees. The risk function shall periodically create awareness amongst the employees in different department / functions on the following aspects:

- Roles & responsibility of employees in management of risks.
- Applicable internal and regulatory risk management guidelines, Key risk indicators and their tolerance limits,
- Risk mitigating controls in place

Roles, responsibility, Powers and Composition:

A - RISK MANAGEMENT COMMITTEE

Purpose

The purpose of the Risk Management Committee (the "Committee") of the Board of Directors (the "Board") of Intellect Design Arena Ltd. (the "Company") shall be to assist the Board in its oversight of the Company's management of key risks, including strategic, financial, operational and compliance risks, as well as the guidelines, policies and processes for monitoring and mitigating such risks. They together constitute the 2nd line of defence

The Committee shall also be responsible for evolving appropriate systems and procedures for ongoing identification and analysis of risks and laying down parameters for efficient management / mitigation of these risks through the Risk Management Policy.

Applicability:

Risk Management Committee shall be applicable to top 1000 listed entities determined on the basis of market Capitalization as at the end of immediate previous year. The Company falls under top 500 listed entities as on March 31, 2021.

Composition of Members:

The Committee shall comprise of the following:

- The Committee shall have minimum three members with majority of them being members of the Board including atleast one Independent Director.
- Senior executives such as Chief Risk Officer, Chief Financial Officer & LoB CEOs may be the members of the Committee as decided by the Board from time to time.

The Committee shall establish a risk management function to be headed by the Chief Risk Officer.

Chairman

The Chairman of RMC shall be a member of the Board of Director as may be decided by the Board from time to time.

Secretary

The Company Secretary shall act as the Secretary to the Committee.

Quorum

The quorum for the Meeting shall be either two members one third of the members of the committee whichever is higher including atleast one member of the Board of directors in attendance.

Conduct of the Meetings

The meetings of the risk management committee shall be conducted in a manner that on a continuous basis not more than one hundred and eighty days shall elapse between any two consecutive meetings.

Minutes

The minutes of the meeting shall be documented and adequately maintained.

Roles & Responsibilities:

The Committee shall assess various risks associated with the business; develop strong risk management systems and risk mitigation strategies and support management and business units in implementing the approved Risk Management Policies and processes, and ensure they are integrated into the business operations and with Internal Control and compliance processes. In addition, the RMC shall also be responsible to:

1. **Establish / Formulate**
    a. Effective Risk Management framework and ensure appropriate methodology, processes & systems are in place to monitor & evaluate risks associated with the business of the organization.
    b. Enterprise Risk Management Policy along with their frameworks and the revisions made time to time.
    c. Risk tolerance limits and assess the cost and benefits associated with risk exposure.

2. **Maintain**
    a. A group wide and aggregated view on the risk profile of the Company for all categories of risk including Business risk, Market risk, Credit risk, Liquidity risk, Operational risk, Information & Cyber Security risk, Compliance risk, Legal risk, Reputation risk, etc.

3. **Review / Monitor**
    a. Monitor & oversee implementation of the risk management policy, including evaluating the adequacy of risk management and internal control systems;
    b. The risk management policy on annual basis, with due considerations to the changing industry dynamics and evolving complexity;
    c. Activities performed to administer companywide Risk Management system & provide necessary guidance.
    d. Company's risk-reward performance to align with overall policy objectives.

e. Solvency position of the Company on a regular basis.
f. Updates on business continuity.
g. Implementation of Anti-fraud policy for effective deterrence, prevention, detection and mitigation of frauds.
h. Discuss & consider best practices in risk management in the market and advise the respective functions.
i. Description of the risk management architecture of the Company to be disclosed as part of the annual accounts.
j. Summary of material risks arising out of vendor contracts annually.

k. Update on the activities of the Company's Information & Cyber Security sub-committee.
l. Significant risks arising out of exceptions to the Information & Cyber security policy.
m. appointment, removal and terms of remuneration of the Chief Risk Officer jointly with the nomination & remuneration committee

4. Report/Advise
To the Board, details on the risk exposures, nature & content of discussions, recommendations and the actions taken to manage the exposures

5. Relationship with Audit

The Risk Management Committee is responsible for coordinating Risk Assessment and updating the Risk framework/register periodically. The assessment findings will be shared with Internal Audit who will use the information to formulate the audit plan.

Internal Audit is responsible for providing independent assurance on internal controls put in place by management on the business processes for specific risks and prevents them from happening. The Risk Management Committee shall work with Internal Audit on identifying internal control weaknesses in relation to the risks identified and coordinating the implementation of control measures.

6. **Others**
The Committee shall have the power to:

a) obtain relevant information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise if it considers necessary engage, remove and reappoint advisors;
b) coordinate its activities with other committees, in case of any overlap with the activities of such Committee

Amendment

Any amendment, modification, alteration in the terms of the policy shall be carried out with the approval of the Board.

Board of Directors:

The Board shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit including cyber security.