Intellect Design Arena Ltd.

Enterprise Risk Management Policy

Note: *Amended ERM Policy — Effective March 3rd, 2026*

Table of Contents

1 Introduction

Intellect Design Arena Ltd. (The Company) is dedicated to upholding transparency, integrity, and accountability in all its interactions with clients, shareholders, associates, distribution partners and regulators. The Company aims for exponential business growth while delivering high quality designs & innovative solutions to clients and maximize returns for the shareholders. Embracing the economic principle of "higher risk can lead to greater rewards", the company recognizes that as its size, scale, and complexity increases, it must engage in calculated risk taking to achieve superior earnings and profitability

Therefore, it is important for the Company to have in place a robust, organized and effective Enterprise risk management systems, processes & technologies.

To this end, the Company has established the Risk Management Policy ("Policy"), which is strategically designed to deepen its expertise in identifying, assessing, and managing enterprise-wide risks. This Policy not only aims to enhance operational efficiency and effectiveness but also serves as a critical framework for fostering a proactive risk culture, ensuring that the organization is well-equipped to navigate uncertainties and seize opportunities in an increasingly complex business environment.

The Policy takes into consideration the regulatory requirements set forth by the key legislation including Information Technology Act, the Companies Act and regulations set forth by Securities and Exchange Board of India (SEBI), as well as local laws and other applicable regulations

- **Information Technology (IT) Act:** This Act mandates the protection of sensitive personal data and information, requiring organizations to implement adequate security practices and procedures to safeguard such data. Compliance with this Act ensures that the Company adheres to necessary data protection standards.

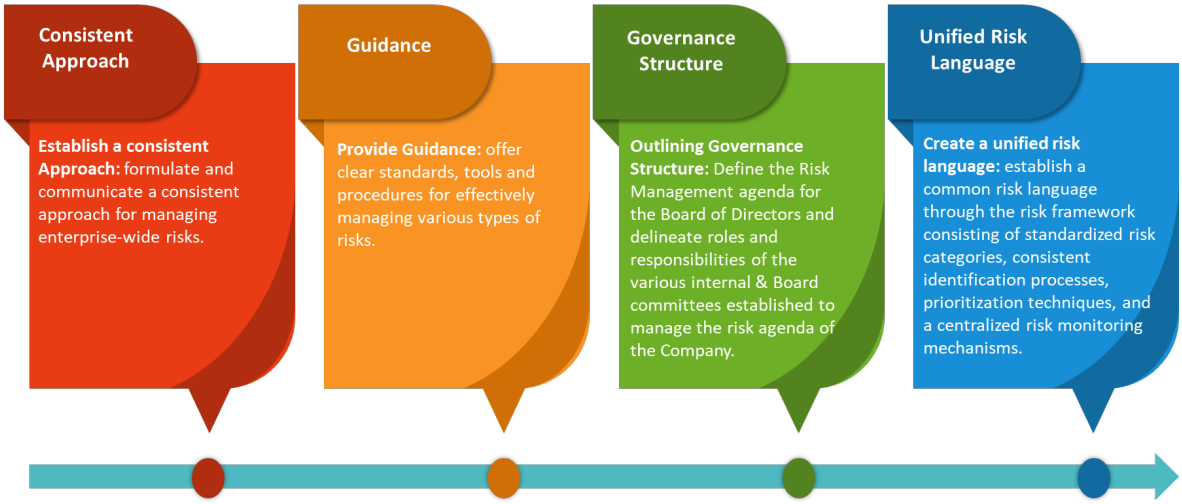
- **Companies Act:** The Companies Act outlines various corporate governance requirements, including the establishment of internal controls and risk management frameworks.

- **Securities and Exchange Board of India (SEBI) Regulations:** SEBI regulations impose requirements for disclosures and compliance for publicly traded companies, emphasizing the need for effective risk management practices.

- **General Data Protection Regulation (GDPR):** For operations involving the EU, compliance with GDPR is crucial. This regulation requires organizations to implement stringent data protection measures.

1.1 Objective

The objectives of the Risk Management Policy are to establish following:



1.2 Policy Scope

The policy is applicable to all functions and departments within the company, encompassing a comprehensive range of risks- both internal and external - to which the organization may be exposed. This inclusive approach ensures that every aspect of the Company's operations is considered in the risk management framework, facilitating a holistic understanding of potential vulnerabilities and opportunities.

2 Risk Management Principles

The Company's risk management policy is designed not only to eliminate risk and volatility but to understand and effectively manage the risk encountered in its operations. The policy is structured around several key components:

1. Risk Identification: The policy mandates a comprehensive identification process for existing and potential risks across the organization. This proactive approach ensures that all possible threats are recognized early, allowing for timely intervention.

2. Risk Assessment: The likelihood and impact of identified risks are assessed through qualitative analysis and expert judgment. This evaluation process helps prioritize risks based on their potential effect on the organization.

3. Risk Mitigation & Response Planning: Risk mitigation and response planning is the crucial next step after risk assessment in the risk management process. It involves developing strategies to address identified risks and minimize their potential impact on the organization. This phase typically includes prioritizing risks based on their severity and likelihood, then creating specific action plans for each significant risk. Common strategies include risk reduction, transfer, and acceptance. The process involves assigning risk owners, determining risk triggers, and outlining detailed response actions.

4. Risk Monitoring & Control: Risk Monitoring and control is an ongoing process that follows risk mitigation and response planning in the risk management lifecycle. It involves continuously tracking identified risks, monitoring risk triggers, and evaluating the effectiveness of implemented risk responses. The phase includes reassessing project risks, conducting risk audits and analysing technical performance.

- **Review of Internal Controls:** A thorough review of the design and operational effectiveness of internal controls is essential. This concludes assessing residual risk exposures within business processes and operational procedures, ensuring that the controls are in place and robust and effective.

5. Communication & Stakeholder Engagement: The policy emphasizes the importance of timely reporting and review of risks by stakeholders and management. The ongoing communication enables informed decision-making regarding mitigation strategies, ensuring all levels of the organization remain aware of current risk profiles.

6. Lessons Learnt: Lessons Learnt is a crucial process in risk management that involves capturing and analysing experiences from past projects and risk events. The primary goal is to extract valuable insights from past experiences to inform future risk management strategies and decision-making processes.

7. Continuous Improvement: Continuous improvement in risk management focuses on ongoing enhancement of risk-related processes, tools, and practices. Key aspects include:

- Regularly reviewing and updating risk management policies and procedures.
- Implementing feedback mechanisms for real-time process refinement.
- Adopting new technologies and methodologies to improve risk assessment and mitigation.
- Benchmarking against industry best practices and standards.

3 Three Layers of Defence

The 3 layers of defence model is a fundamental framework for effective risk management within the Company, delineating clear roles and responsibilities across different organizational levels to ensure comprehensive risk oversight and control.

By clearly defining these three layers of defence, the Company aims to establish a cohesive approach to risk management that enhances transparency, accountability, and resilience across all the levels of organization.

3.1 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. This is crucial as it integrates controls directly into systems and processes, supported by adequate managerial and supervisory check to ensure compliance. It serves to promptly identify control breakdown, inadequate processes, and unexpected events, thereby empowering functional management to own and manage their risks effectively. **[Functions Own and manage their risks – Functional Management].**

3.2 Second Line of Defence

The second line of defence comprises risk management and compliance functions that support and monitor the implementation of effective risk management practices by operational management. This layer assists risk owners in defining their risk exposures and ensures the reporting of relevant risk information across the organization. Oversight is provided by the Risk Management Committee, the Chief Risk Officer, and other risk management personnel, who collaborate with functional counterparts to uphold a robust risk framework. This layer is crucial in ensuring that the first line of defence adheres to established risk policies and procedures. **[Function that provides/conducts Oversight & Internal Monitoring of Risks – Risk Management, Compliance and other Control/Assurance functions].**

3.3 Third Line of Defence

The third line of defence is represented by the internal audit function, which provides independent assurance regarding the effectiveness and integrity of the company's systems and processes. This layer evaluates the design and implementation of risk management practices across the organization, ensuring that both the first and second lines of defence operate effectively. By delivering objective assessments, the internal audit function reinforces accountability and fosters continuous improvement in risk management practices. **[Function that provides independent assurance – Internal Audit].**

4 Risk Governance Structure

Intellect has established a robust risk governance structure anchored in its BELIEF framework (Brand, End Customer, Leadership, Intellectual Property, Execution, Financial), which guides the Board of Directors in overseeing enterprise-wide risk management. The system integrates layered accountability, structured committees, and proactive risk assessment tools to balance innovation with stability.

4.1 Board of Directors

The Board of Directors shall establish robust systems to regulate the Company's risk profile. To cultivate a strong risk management framework and develop effective mitigation strategies, the Board recognizes the importance of addressing the diverse range of risks to which the Company is exposed.

The Board of Directors holds the fundamental responsibility to establish and maintain robust systems that effectively regulate the Company's risk profile. This critical function involves:

1. **Strategic Oversight**
   - Setting appropriate risk thresholds aligned with business objectives
   - Defining clear risk tolerance levels across all operations
   - Regularly reviewing and adjusting risk parameters

2. **Framework Development**
   - Implementing comprehensive risk management strategies
   - Creating effective mitigation approaches
   - Ensuring alignment with industry best practices
   - Adapting to evolving business environments

3. **Risk Assessment**
   - Strategic risks affecting long-term objectives
   - Operational risks impacting daily functions
   - Financial risks concerning market and economic factors
   - Compliance risks related to regulatory requirements
   - Reputational risks affecting brand value

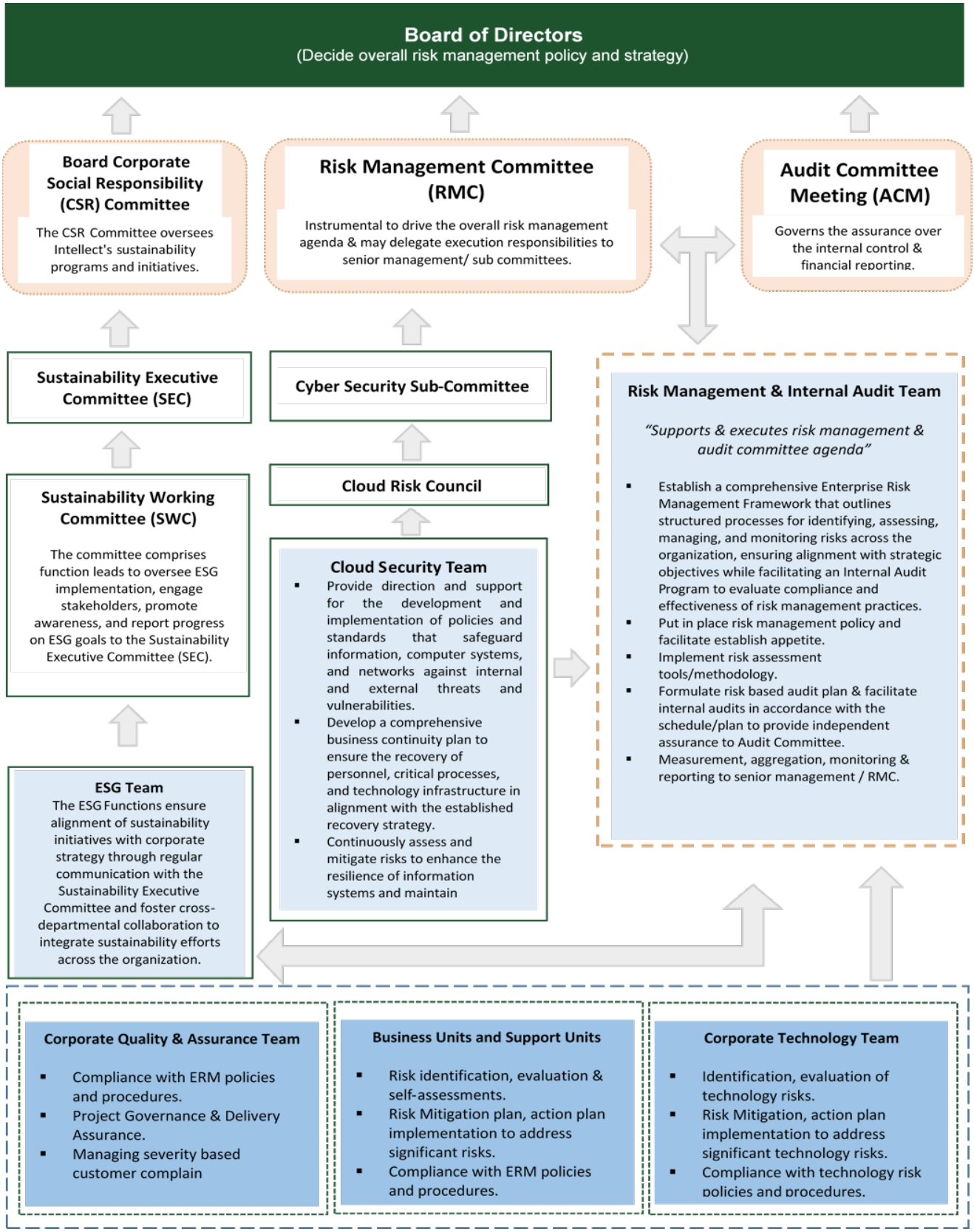
To this end, the Board has implemented a comprehensive governance structure that facilitates proactive risk oversight and ensures effective identification, assessment, and management of potential risks. This robust framework not only supports the Company in achieving its strategic objectives but also fosters a culture of risk awareness and accountability throughout the organization:

1. **Risk Management Committee (RMC) -** RMC plays a central role in overseeing the company's overall risk management framework.

2. **Audit Committee Meeting (ACM) -** The Audit Committee focuses on financial risks and internal controls, complementing the work of the Risk Management Committee.

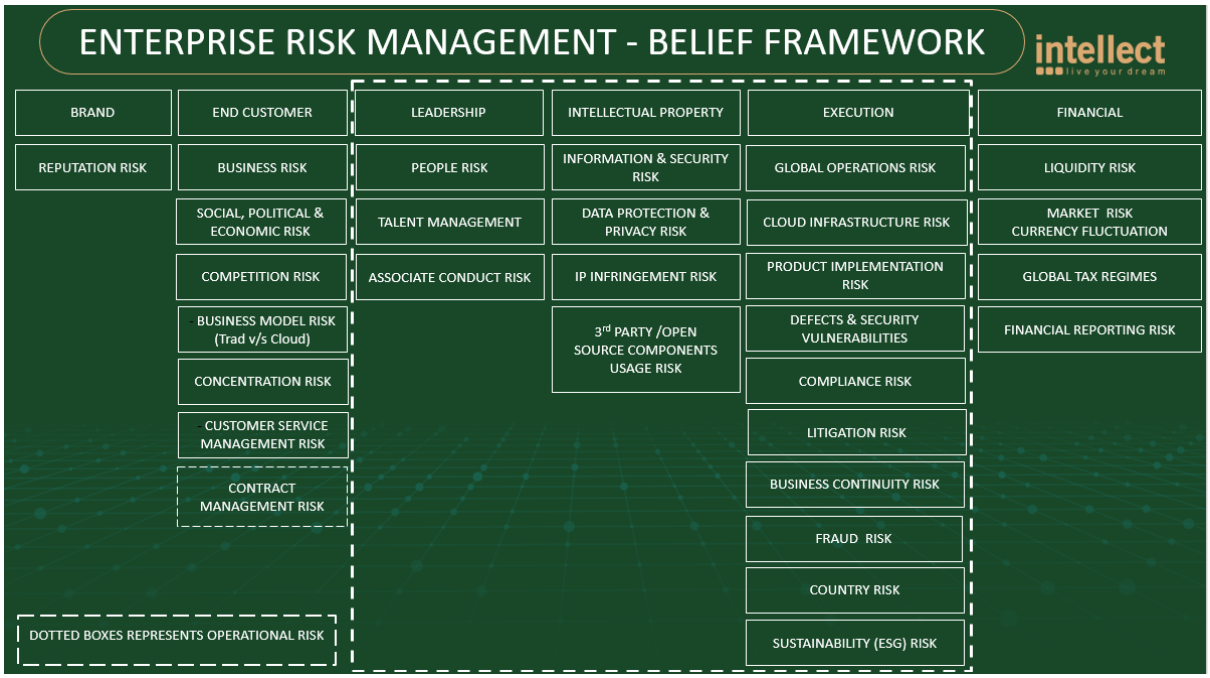
3. **Corporate Social Responsibility (CSR) Committee & Sustainability Executive Committee (SEC)** - The CSR and SEC committee primarily focuses on managing risks related to the company's social and environmental impact.

4.2 Governance Structure



4.3 BELIEF Framework

The BELIEF framework is a strategic risk management architecture that consolidates organizational risks into a cohesive structure. The framework's distinctive strength lies in its integrated approach, connecting various risk categories into a unified system that enables comprehensive risk identification, assessment, and mitigation while maintaining organizational resilience and growth objectives. This framework, which stands for Brand, End Customer, Leadership, Intellectual Property, Execution, and Finance, offers a holistic view of potential risks across various aspects of the business.



The framework's effectiveness stems from several key attributes:

1. **Strategic Alignment:** The framework aligns risk management with business objectives by covering both operational and strategic risks.
2. **Holistic Coverage:** It addresses risks across all critical business functions, from brand reputation to financial operations.
3. **Hierarchical Structure:** The clear categorization allows for systemic risk identification, assessment and mitigation.
4. **Operational Integration:** By segregating into specific categories, it enables targeted control measures and monitoring.

4.3.1 Why is the BELIEF framework needed?

The BELIEF framework is uniquely suited to Intellect's needs as a global leader in financial technologies. It provides a comprehensive, industry-specific approach to risk management that aligns with the company's strategic initiatives, protects its core assets, and addresses the complex risk landscape of the financial technology sector. This tailored approach

enables Intellect to maintain its competitive edge while managing the diverse risks inherent in its business operations.

- **Industry-Specific Tailoring -** Intellect operates in the financial technology sector, which faces unique challenges and risks. The BELIEF framework is specifically tailored to address the complexities of this industry:
  - **Financial Technology Focus**
    - Addresses risks associated with cutting-edge financial products and services.
    - Emphasizes intellectual property protection, crucial in the fast-paced FinTech environment.
    - Incorporates cloud and data privacy risks, which are paramount in financial technology.
  - **Global Operations Consideration**
    - Accounts for risks associated with operating in multiple jurisdictions.
    - Addresses currency fluctuation risks, essential for a company with international presence.
    - Includes compliance risks, critical in the heavily regulated financial services sector.

- **Holistic Risk Integration -** The BELIEF framework stands out by integrating various risk categories that are often managed separately in traditional risk management approaches:
  - **Brand and Customer Integration**
    - Uniquely combines brand risks with customer risks, recognizing their interconnectedness in the FinTech space
    - Acknowledges that customer trust and brand reputation are intrinsically linked in financial services
  - **Leadership and Talent Focus**
    - Emphasizes leadership risks, including succession planning and talent management.
    - Recognizes the critical role of human capital in driving innovation and maintaining competitive edge in FinTech.

- **Strategic Alignment -** The framework aligns closely with Intellect Design Arena's business strategy and core competencies:
  - **Intellectual Property (IP)**
    - Highlights the importance of protecting intellectual property, a key asset for a company positioning itself as an agenda-setter in FinTech.
    - Includes specific categories for information security and source code control, crucial for maintaining competitive advantage.
  - **Execution Risk Management**
    - Incorporates product implementation risks, reflecting the company's focus on innovative product development.
    - Addresses cloud risks, aligning with the company's cloud-based service offerings.

- **Comprehensive Financial Risk Coverage -** The framework provides an extensive approach to financial risk management.
  - **Multifaceted Financial Risk Approach**
    - Covers a wide range of financial risks including credit, market, and currency fluctuation risks.
    - Incorporates financial reporting risks, essential for maintaining investor confidence and regulatory compliance.

- **Adaptability and Future-Proofing - The** BELIEF framework is designed to be adaptable to evolving business landscapes:
  - **Emerging Risk Categories**
    - Includes modern risk categories like data privacy and cloud risks, demonstrating foresight in risk management.
    - Flexible structure allows for the incorporation of new risk categories as they emerge.

4.3.2 How does the BELIEF framework compare to other risk frameworks?

The BELIEF framework, which categorizes risks into Brand, End Customer, Leadership and Intellectual Property, Execution, and Finance, offers a unique approach to risk management compared to other established frameworks.

- **Comprehensive categorization**

The BELIEF framework provides a holistic view by categorizing risks into specific areas that are crucial to the organization's success. This contrasts with frameworks like **ISO 31000**, which emphasizes a more general approach to risk management without specific categories, allowing for broader application across various industries.

- **Focus on stakeholder perspective**

Unlike frameworks like **COSO**, which primarily focuses on internal controls and governance structures, the BELIEF framework includes external factors (like Brand capital) that directly impacts organizational performance This stakeholder approach centric approach helps Company align their risk management strategies with their marker positioning and customer expectations.

- **Integration with business strategy**

The BELIEF framework emphasized the integration of risk management with business strategy, similar to the RIMS framework, which promotes stakeholder engagement and strategic alignment. However, the BELIEF framework uniquely highlights specific operational areas (e.g. Execution and Leadership) that are essential for achieving strategic objectives.

- **Quantitative vs Qualitative**

Many traditional frameworks like **FAIR** focus heavily on quantitative analysis of risks, providing detailed metrics for financial implications. In contrast, qualitative assessments

(such as brand & reputation) and quantitative evaluations (like financial risks e.g., liquidity), offer a balanced perspective on the risk management.

- **Operational emphasis**

The BELIEF framework places significant emphasis on operational execution risks, which is crucial for organizations that rely heavily on effective operational processes. This focus is somewhat mirrored in frameworks like **NIST SP 800-37**, which emphasizes compliance and operational security but may not address broader business risks as comprehensively as BELIEF Framework.

In summary, the BELIEF framework stands out by offering a structured but yet flexible approach that integrates various dimensions of risk management while emphasizing stakeholder perspectives and operational effectiveness. Its categorization into specific risk areas allows organizations to tailor their risk management strategies effectively, ensuring alignment with both internal capabilities and external market dynamics. This makes it a valuable tool for the organization seeking a comprehensive understanding of the risk landscape while maintaining agility in their risk management practices.

5 BELIEF Framework - Risk Definitions

5.1 BRAND

From Intellect's perspective, "Brand" represents the company's cumulative market identity and perception as a leading global financial technology solutions provider. "Brand" element represents not just market recognition and trust, but serves as a crucial determinant of the company's ability to maintain stakeholder confidence, secure partnerships with financial institutions, attract talent and sustain competitive advantage in the dynamic financial technology landscape.

"Brand" element in the Enterprise Risk Management Belief Framework occupies a strategic position in the top tier, signifying its fundamental role in:

- Trust and reliability in handling financial transactions.
- Innovation leadership in digital transformation solutions.
- Global delivery capabilities across world markets
- Domain expertise in BFSI sector

Reputational Risk represents the potential impact on Intellect Design Arena's market standing and stakeholder trust arising from adverse events, negative publicity, or service delivery issues that could affect client relationships, market perception, and business sustainability across the global financial technology ecosystem.

5.1.1 Reputational Risk

As a global leader in financial technology solutions, Intellect recognizes the critical importance of managing reputational risks in today's fast-paced and interconnected environment. Reputational Risk, the potential for loss arising from negative publicity, can stem from various sources such as operational failures, cybersecurity breaches, regulatory non-compliance, or poor customer service, and can have far-reaching consequences. Even minor incidents can escalate into significant reputational risk incidents potentially leading to customer exodus, diminished brand equity and financial repercussions. The advent of social media has amplified this risk, enabling negative information to spread rapidly and globally, potentially triggering "reputation damage".

For Intellect, maintaining a strong reputation is not just about preserving its market position, but also about upholding the integrity of the financial ecosystem it serves, making proactive reputation risk management an integral part of its overall risk mitigation strategy.

Intellect identifies several key factors that can contribute to reputational risk:

❖ **Business Practices and Customer Interactions**

- Unethical or questionable business practices can quickly damage reputation.
- Customer complaints arising from product performance issues, poor service quality, or misaligned expectations can significantly impact reputation.
- Delivery failures, including missed deadlines, implementation issues, and integration

challenges, can erode client trust and lead to reputational damage.

❖ **Financial and Communication Factors**

- Subdued financial results or negative investor perceptions can harm reputation.
- Unmeasured press statements or mishandled public relations can damage the organizational image.

❖ **Product and Internal Factors**

- Problems with software products or services can significantly impact reputation in the Fintech industry.
- Associate misconduct, inappropriate social media presence, and cultural misalignment can lead to negative publicity.

❖ **Commercial and Legal Issues**

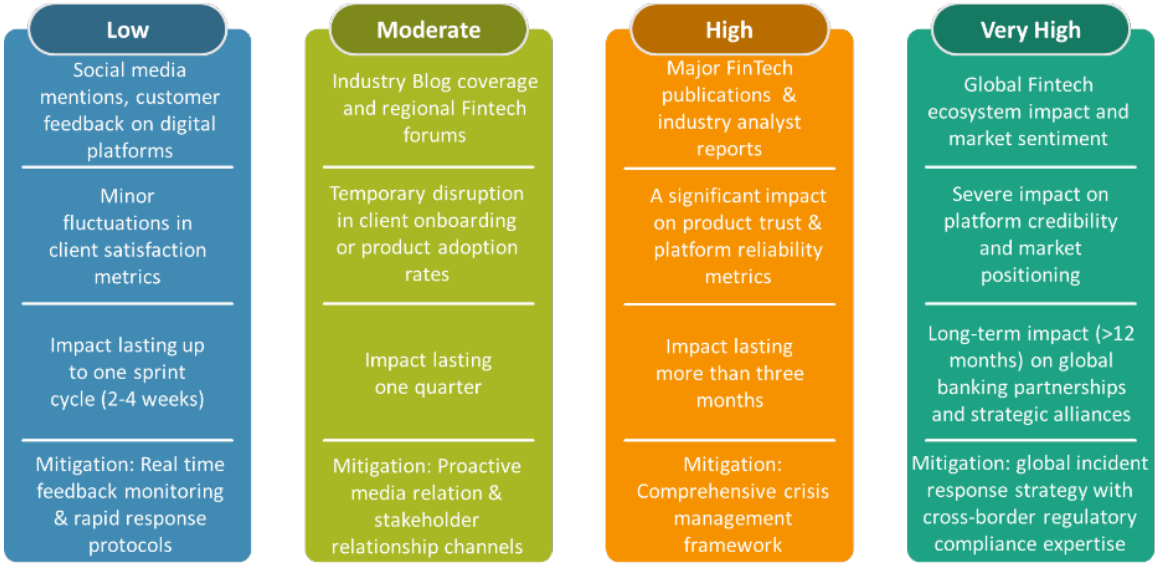
- Disputes arising from client agreements, vendor relationships, or ongoing litigation can create negative perceptions and uncertainty.
- Non-compliance with industry regulations, ethical violations, and lack of transparency can result in fines, penalties, and reputational harm.

❖ **External Perceptions**

- Inter-client feedback and industry perceptions play a crucial role in shaping the company's reputation.

5.1.2 Reputational Risk Mitigation - General Guideline

The below guideline outlines a tiered reputational impact matrix tailored for Intellect, categorizing severity levels (Low to Very High) based on source, duration, business impact, and required mitigation strategy.



5.2 END CUSTOMER

In the BELIEF framework, an “END CUSTOMER” embodies the ultimate beneficiary of Intellect’s comprehensive suite of solutions and services, representing banks, financial institutions, and insurance companies that leverage these technologies to serve their own clientele. This pivotal position at the top of the risk hierarchy pyramid demonstrates their fundamental importance in shaping the entire risk landscape.

“END CUSTOMER” requirements, satisfaction levels, and operational needs cascade downward through multiple risk tiers, creating an intricate web of interdependencies that affects everything from core business strategies to technological architecture choices between traditional and cloud deployments. Their influence permeates through concentration patterns, competitive dynamics, product development investments, contractual frameworks, and potential legal exposures, making them the primary catalyst in the company's risk assessment and mitigation strategies.

The hierarchical risk structure shows how End Customer considerations cascade through multiple risk layers in financial technology operations. End Customers' changing needs, preferences, and behaviours directly impact:

5.2.1 Business Risk

This is the risk of failing to meet customer requirements and evolving preferences, which may result in an inability to generate adequate revenue or lead to losses. Such risks arise from business uncertainties including failure to execute business plans, unforeseen market events, shifts in consumer demand, intensifying competition, business concentration, or product and service obsolescence, potentially leading to business underperformance or failure.

From Intellect's perspective, Business Risk encompasses a multifaceted challenge in the financial technology landscape. There are multiple potential profit uncertainties through several key dimensions:

❖ **Market Dynamics**

- Technology disruption requires continuous upskilling of existing talent to meet evolving customer and market expectations.
- Competition from multinational companies, local players, and Indian product companies, including potential disruption from start-ups.

❖ **Geographic concentration risks**

- Product Portfolio - Specialized focus in BFSI space with four key sub-segments: Corporate Banking, Retail Banking, Capital Markets, and Insurance.
- Risk mitigation through diversification into various payment businesses.

❖ **Innovation & Adaptation**

- Continuous investment in innovative solutions is crucial to stay ahead in the market competition.
- Challenge in building and hardening technology stacks to meet regulatory security requirements while maintaining innovation pace.
- Risk of product obsolescence requires constant evaluation.

5.2.2 Business Risk Mitigation - General Guideline

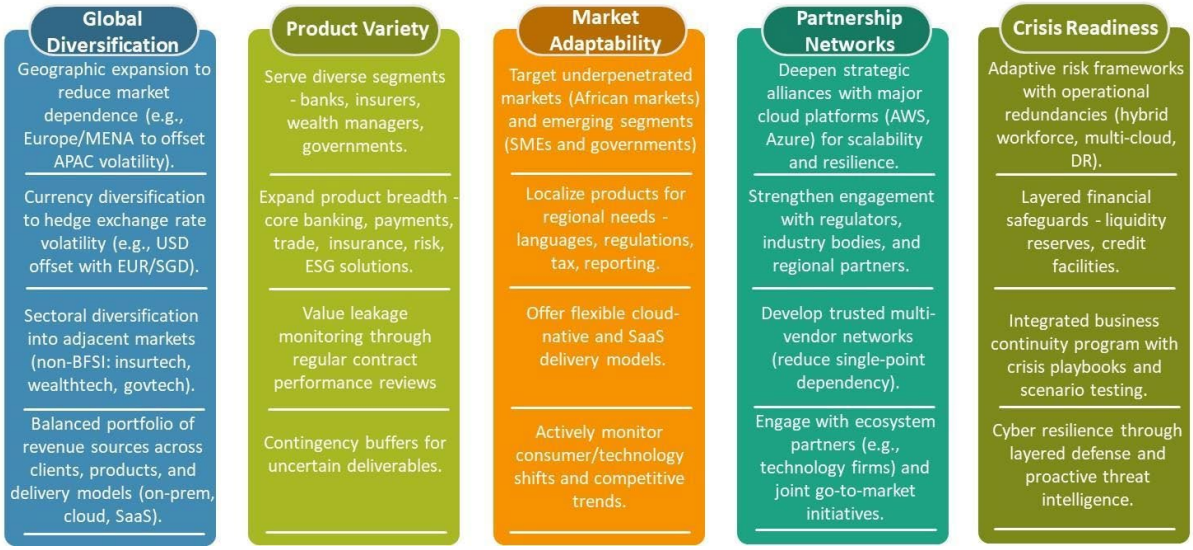
The matrix below summarizes a strategic framework for business risk mitigation through four pillars - Strategic Diversification, Product Innovation, Market Positioning, and Customer Engagement, each offering targeted controls to enhance resilience and growth adaptability.

5.2.3 Social, Political & Economic Risk

Intellect Design Arena faces risks from economic instability (like market fluctuations, geo-political tensions, inflation, or pandemics) and shifts in consumer behaviour (such as changing preferences in technology or financial services). These factors could pressure the financial sector to cut costs or reduce demand for Intellect's products.

5.2.4 Social, Political & Economic Risk Mitigation - General Guideline

The matrix below summarizes general mitigation controls across five strategic pillars, designed to enhance organizational resilience, scalability, and responsiveness to evolving market and operational risks.



5.2.5 Competition Risk

Intellect operates in a dynamic financial technology sector where competition risk refers to the potential loss of market share, profitability, or strategic positioning due to actions by competitors, structural market shifts, or regulatory changes impacting competitive dynamics.

Key structural factors defining Competition Risk in financial technology landscape are:

❖ **Competitive Pressures**

- Although Intellect is uniquely placed in terms of its overall product portfolio and business offerings, it does compete with other firms in individual segments. The banking technology market, growing at a rapid pace, intensifies competition as these firms vie for digital transformation projects.
- New entrants with lower overheads and innovative business models can disrupt established players by offering more agile and cost-effective solutions.

❖ **Technological Disruption and Standardization**

- The fast pace of technological change in areas like AI, block chain, and cloud computing

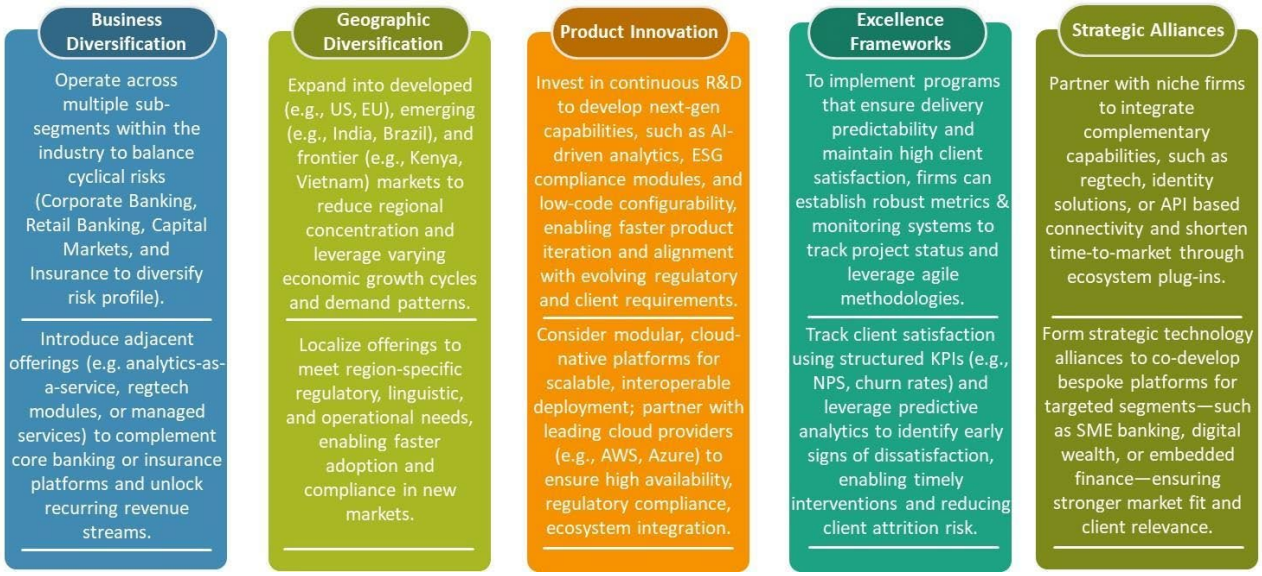
requires continuous investment and adaptation to remain competitive. Failure to adapt risks obsolescence

❖ **Data control & cybersecurity threats**

- Access to customer data is a competitive battleground. Firms controlling large datasets may engage in exclusionary practices, such as denying competitors access.
- Centralized platforms (e.g., payment gateways) are prime targets for breaches, risking reputational damage and regulatory penalties.

5.2.6 Competition Risk Mitigation - General Guideline

The matrix below summarizes general mitigation controls designed to strengthen business resilience, agility, and strategic alignment across key operational and market dimensions.



5.2.7 Model Risk

Model risk, for Intellect, arises from potential failures in adapting its product offerings, pricing models, or operational strategies to align with industry shifts toward cloud-based solutions and emerging technologies. Key risk drivers include:

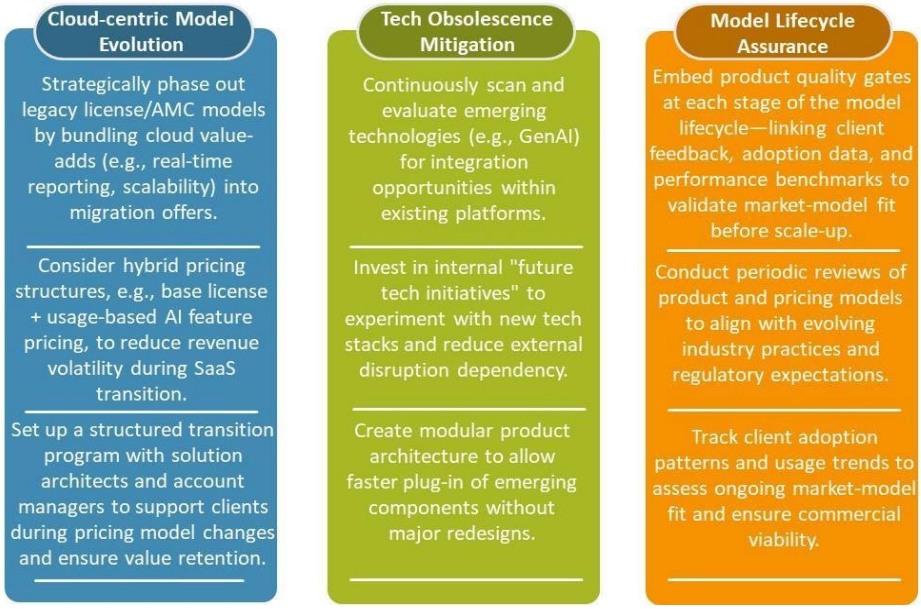
❖ **Cloud Transition Risks:** Moving from traditional license/AMC models to SaaS/subscription-based revenue streams may destabilize legacy revenue pipelines.

❖ **Technology Disruption:** Innovations like AI/ML, big data analytics, and Internet of Things (IoT) could render existing products obsolete if not integrated proactively.

❖ **Market Relevance:** Competitors leveraging cloud-native architectures and digital-first strategies may erode Intellect's market share in core BFSI sectors.

5.2.8 Model Risk Mitigation - General Guideline

The matrix below summarizes model risk mitigation controls tailored for Intellect addressing key vulnerabilities arising from cloud transition, technology obsolescence, and lifecycle misalignment between product offerings and evolving market expectations.



5.2.9 Concentration Risk

Concentration Risk refers to the potential for significant financial or operational loss arising from over-reliance on a single client, market segment, technology, or geographic region. For Intellect, this risk manifests in four core dimensions:

❖ **Client Concentration**

Over-dependence on a few large financial institutions for revenue. For instance, losing a major client could significantly impact revenue streams.

❖ **Sectoral Concentration**

Sector-wide downturns directly affect growth. Intellect deals in BFSI (Banking, Financial Services, Insurance), which constitutes ~85% of its client base.

❖ **Technological Concentration**

Reliance on proprietary platforms (like iTurmeric and eMACH.ai), while innovative, creates vendor lock-in risks if competitors adopt alternative standards.

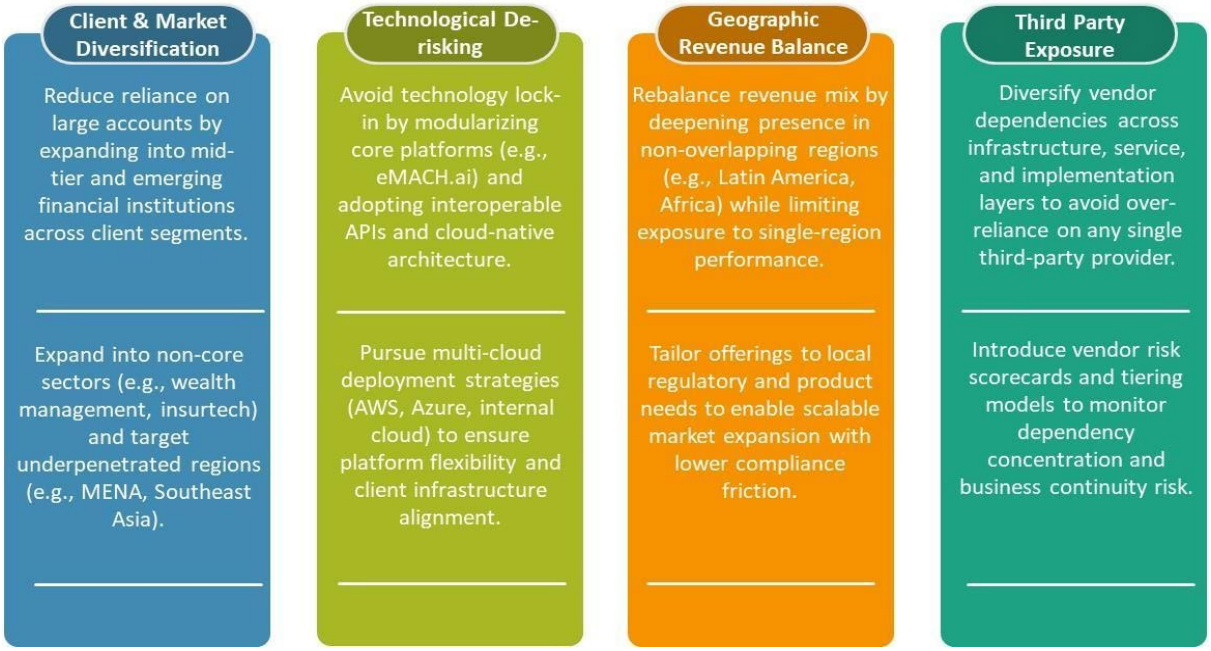
❖ **Geographic Concentration**

A substantial reliance on revenue from a specific geographic region may expose an organization to heightened political and economic vulnerabilities. In such cases, geopolitical instabilities or economic contractions within that area could potentially result in adverse

effects on the company's income flows. This concentration of revenue sources in a particular locale amplifies the risk profile, as regional fluctuations in political climate or economic conditions can disproportionately impact the organization's financial performance.

5.2.10 Concentration Risk Mitigation - General Guideline

The matrix below summarizes key risk mitigation strategies across four critical dimensions, client and market diversification, technological de-risking, geographic revenue balance, and third-party exposure, to strengthen organizational resilience and reduce operational vulnerabilities.



5.2.11 Customer Service Management Risk

Intellect's reliance on long-term contracts with clients across diverse jurisdictions introduces multifaceted risks tied to compliance, operational alignment, and relationship sustainability.

Contractual & Compliance Risks

- **Fragmented Regulatory Compliance:** Differing legal frameworks (e.g., GDPR in Europe vs. RBI guidelines in India) create compliance gaps.
- **Cross-Jurisdictional Conflicts:** Dispute resolution becomes complex when contracts span regions with conflicting laws (e.g., U.S. vs. ASEAN arbitration norms).
- **Vendor Lock-In:** Over-dependence on rigid contractual terms limits adaptability to client-specific needs or market shifts.

Operational & Relationship Risks

- **Performance Misalignment:** Standardized terms may not reflect unique client deliverables, leading to disputes (e.g., API uptime, SLAs vs. actual cloud performance).

- **Customer Attrition:** Poor relationship management risks losing clients contributing >15% of revenue.
- **Communication Breakdowns:** Cultural/language barriers (e.g., MENA vs. APAC clients) can delay issue resolution.

Market & Sectoral Risks

- **Economic Concentration:** Over-reliance on BFSI clients (85% revenue) exposes Intellect to sectoral downturns (e.g., 2023 EU banking crisis).
- **Technological Obsolescence:** Legacy platforms risk displacement by AI/cloud-native competitors.

Technological & Innovation Risks

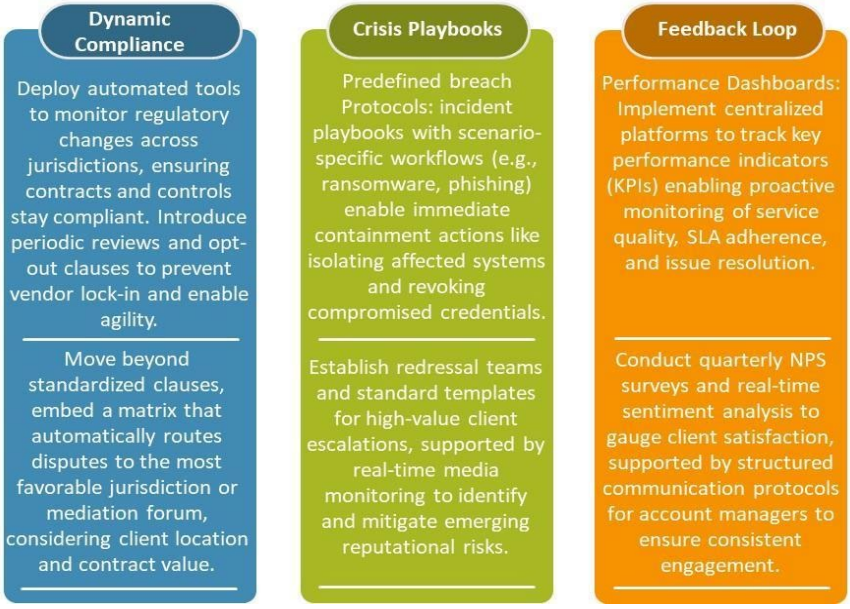
- **Integration Challenges:** Legacy systems struggle with API-heavy Fintech ecosystems.
- **Cybersecurity Threats:** Centralized platforms (e.g., payment gateways) attract breaches, risking penalties up to 4% of global turnover under GDPR.

Reputational Risks

- **Publicized Breaches:** A single compliance failure could erode trust in clients.
- **Contractual Disputes:** Prolonged litigation (e.g., delayed project delivery) harms brand equity.

5.2.12 Customer Service Management Risk Mitigation - General Guideline

The matrix below summarizes key risk management mitigation controls for customer service operations, focusing on proactive compliance, incident response, and continuous improvement to enhance resilience and client satisfaction.



5.2.13 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.

Contract risk in Intellect Design Arena's context encompasses multiple dimensions that affect the organization's ability to deliver and maintain business deliverables:

Financial Impact

- Value leakage from poor contract processes and unapproved pricing models.
- Potential losses from missed renewal deadlines and automatic renewals.
- Cost overruns from inadequate performance tracking and scope creep.

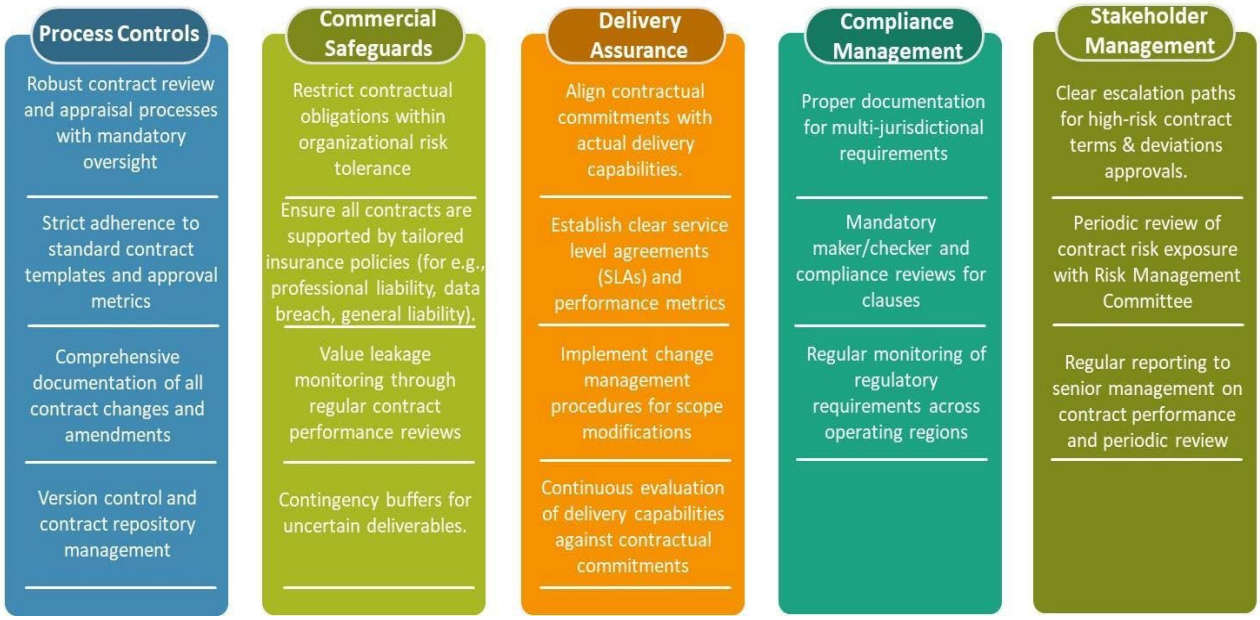
Operational Impact

- Risk of non-delivery or subpar performance against contracted service levels.
- Challenges in meeting delivery timelines and quality expectations.
- Misalignment between organizational capabilities and contractual commitments.

Deviations

- Accepting liability and indemnity terms beyond organizational thresholds and tolerance.
- Committing to deliverables outside standard product capabilities.
- Non-compliance with prescribed approval matrices for deviation's approval/sign-offs.
- Non-adherence to change management procedures & version controls.

5.2.14 Contract Risk Mitigation - Guidelines



5.3 LEADERSHIP

In the BELIEF framework, leadership serves as the foundational thread connecting people risk, talent management, and associate conduct risk through governance structures, cultural norms, and strategic alignment. Leadership directly shapes talent management by aligning workforce strategies with organizational resilience goals (e.g., addressing skill gaps or succession planning) and mitigates people risk by fostering ethical practices and psychological safety to reduce attrition or burnout. For associate conduct risk, leadership enforces accountability frameworks and cultivates a risk-aware culture.

5.3.1 People Risk

Risks arising from gaps in talent management, succession planning, or employee misconduct, which can disrupt operations, harm reputation, or reduce competitiveness.

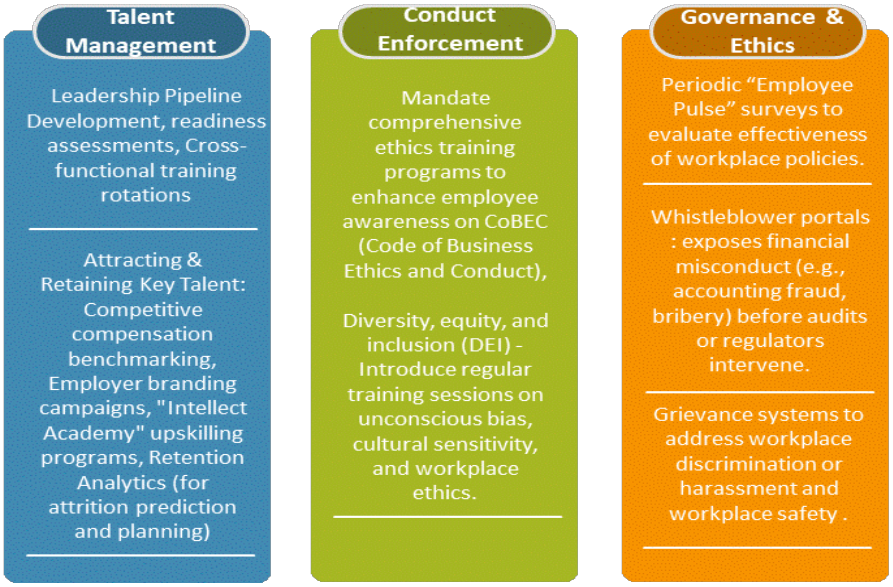
5.3.2 Talent Management

Risks pertaining to the ability to attract or retain top or key talent with specialised skill sets for the organisation.

5.3.3 Associate Conduct Risk

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.

5.3.4 People Risk Mitigation - General Guideline



5.4 INTELLECTUAL PROPERTY

Intellectual Property (IP), from a risk management perspective, involves safeguarding intangible assets against key vulnerabilities. These include Information & Security Risk, where sensitive IP data may be exposed to breaches or theft; Data Protection & Privacy Risk, which arises from mishandling proprietary or personal data, potentially leading to legal and reputational damage; IP Infringement Risk, involving unauthorized use or duplication of protected IP; and Third-Party/Open Source Components Usage Risk, where improper compliance with licensing agreements for external components can result in liabilities.

Effective management of these risks is essential to protect IP and maintain its value.

5.4.1 Information & Cyber Security Risk

Threats from malicious actors (internal/external) targeting IT infrastructure, data assets, or personnel, which could lead to:

- Unauthorized data exfiltration (e.g., customer PII, trade secrets)
- Disruption of business operations (e.g., ransomware, DDoS attacks)
- Source code theft or tampering (e.g., unauthorized access to repositories)
- Reputational damage from publicized breaches or regulatory penalties (e.g., GDPR fines)

❖ **Governance Mechanism**

- Cross-functional Information & Cyber Security Forum overseeing threat intelligence sharing and policy enforcement.
- Annual ISO 27001/27017/27018, PCI DSS, and SOC 2 audits to validate controls for cloud security, data privacy, and payment systems.

❖ **Technical Safeguards**

- Network segmentation, zero-trust architecture, and endpoint detection tools.
- Multi-layered encryption (data-at-rest and in-transit).

❖ **Risk Transfer**

- Cyber liability insurance covering forensic investigations, legal fees, and breach notifications.

5.4.2 Data Protection & Privacy Risk

Inadequate safeguards for sensitive data (customer/employee), leading to:

- Non-compliance with evolving regulations (e.g., GDPR, CCPA, India's DPDP Act)
- Fines or sanctions for improper cross-border data transfers
- Loss of stakeholder trust due to misuse of AI/ML-driven customer analytics

❖ **Process Controls**

- Data Authorization Framework: Role-based access controls (RBAC) and just-in-time (JIT) privileges.
- GDPR Compliance Reviews: Mapping data flows, conducting DPIAs (Data Protection

Impact Assessments), and appointing DPOs.

❖ **Technical Tools**

- VAPT/DAST: Automated vulnerability scans integrated into CI/CD pipelines.
- Tokenization/anonymization for unstructured data repositories.

5.4.3 Intellectual Property Right (IP) Infringement Risk

Intellectual Property (IP) risk refers to the potential threats and vulnerabilities that could lead to loss, infringement, misappropriation, or unauthorized use of Intellect Design Arena's proprietary assets, including patents, trademarks, copyrights, trade secrets, and software codes. These risks can arise from external threats such as competitors, counterfeits, cybercriminals, or internal risks including non-compliance with licensing agreements, misuse of open-source software, or employee negligence. Failure to manage IP risks can result in financial losses, legal disputes, reputational damage and operational disruptions.

a) Protection of Intellectual Property (IP)

The company's intellectual property including proprietary algorithms, software platforms, data models, trademarks, and other intangible assets, forms a cornerstone of its competitive advantage and revenue generation model. Given the cross-border nature of fintechs, ensuring consistent and enforceable IP protection across jurisdictions can be challenging. The risk of infringement or misappropriation is mitigated through a multi-pronged approach including:

- Registration and enforcement of IP rights in key geographies with robust legal frameworks and enforceable IP laws.
- Implementation of internal controls and oversight mechanisms to safeguard proprietary assets.
- Ongoing monitoring for potential violations or unauthorized usage.
- Engagement with external legal advisors for proactive risk identification and timely enforcement of IP claims

This framework ensures that the Company's intellectual property is adequately protected, enabling sustained innovation and value creation.

b) Risk of use of "Open Source" Software

The company leverages Open Source Software (OSS) in select product and service offerings to accelerate innovation and reduce development costs. However, failure to comply with the licensing terms associated with OSS such as attribution requirements, distribution constraints, or reciprocal licensing clauses may expose the company to legal, financial, and reputational risks.

To mitigate this risk, the company has adopted a formal Open Source Software Usage Policy that outlines clear procedures for:

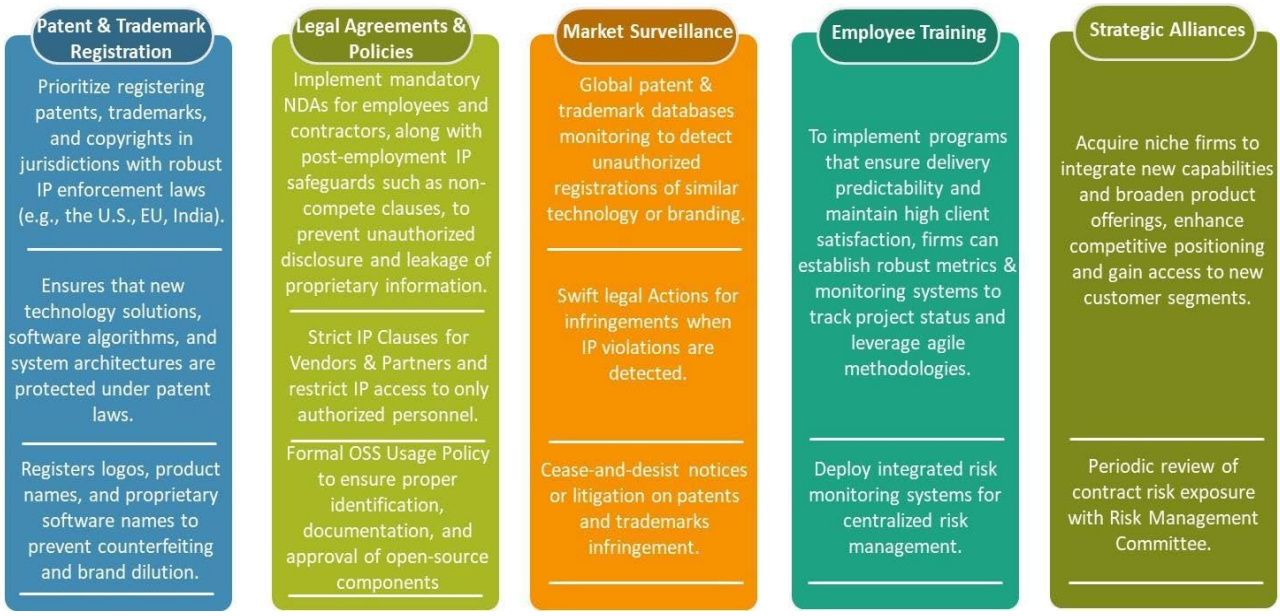
- Identification, documentation, and approval of OSS components during the software development lifecycle,
- Regular monitoring and review of license obligations by the IT and Legal teams,
- Centralized oversight through mandatory reporting by business units to the IT department for all OSS and Free and Open Source Software (FOSS) usage
- Education and periodic training of developers and technology teams on OSS compliance

In addition, usage of Commercial Off-The-Shelf (COTS) software is governed by formal licensing agreements and is subject to periodic audits by the IT department to ensure license validity, usage limits, and adherence to contractual terms. Together, these controls support responsible adoption of third-party software, minimize infringement risks, and ensure compliance with both legal requirements and internal governance standards.

5.4.4 IP Risk Mitigation - General Guideline

Intellect Design Arena's proprietary technologies, software solutions, and patents form the core of its competitive advantage. However, protecting these assets presents significant challenges:

- **Unauthorized use or Copying:** Competitors, former employees, or third parties may attempt to replicate or misuse proprietary technology, leading to loss of market exclusivity.
- **Legal Challenges & Litigation:** Weak IP enforcement could result in prolonged legal disputes, financial liabilities, and injunctions restricting product sales.
- **Jurisdictional Differences:** IP protection laws vary across countries, making enforcement difficult in regions with weaker regulatory frameworks.



5.5 EXECUTION

Execution Capital refers to the organization's institutional capacity to deliver on its strategic objectives, client commitments, and operational goals in a consistent, scalable, and controlled manner. It encompasses the effectiveness of internal program governance, the agility of execution processes, the adequacy of resource allocation, and the resilience of delivery mechanisms.

Under the BELIEF framework, Execution Capital is not measured in financial terms but in the organization's ability to translate strategy into successful outcomes through disciplined execution. It reflects the maturity of our program management practices, readiness to adapt to dynamic client and regulatory requirements, and our capability to identify, monitor, and mitigate delivery-related risks across functions.

5.5.1 Global Operational Risk

The organisation's global operations may be impacted by a range of factors inherent to international business activities and jurisdictional differences.

These include, but are not limited to:

- Varying laws and regulations in the banking and financial services sector.
- Divergent work practices, such as remote working norms and labour regulations.
- Complex and evolving tax regimes, licensing requirements, and cross-border compliance obligations.
- Trade barriers, tariff structures, and differences in corruption perception and enforcement standards.

- Data protection and privacy laws, which may differ significantly across regions.
- Geopolitical risks, such as international embargoes, sanctions, hostilities, terrorism, armed conflicts, mass migration, and political instability.
- Immigration and staffing challenges, including skilled workforce mobility and visa restrictions.

5.5.2 Global Operational Risk Mitigation – Guidelines

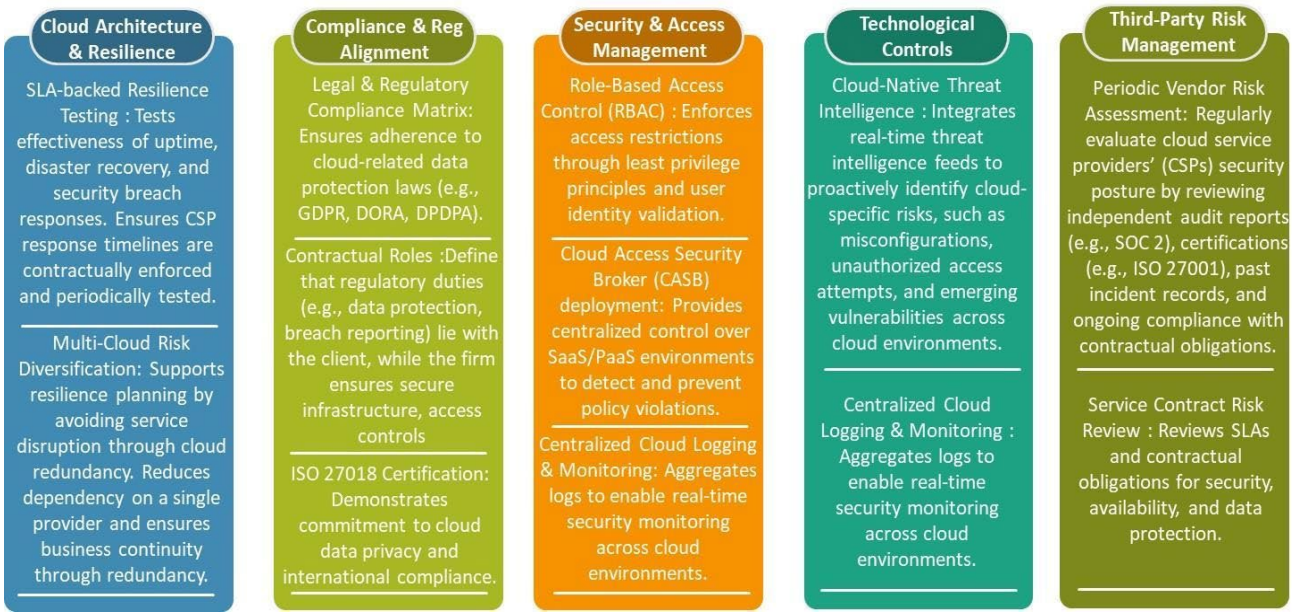
The matrix below summarizes key risk management mitigation controls for global operational risk, highlighting essential measures across regulatory compliance, operational continuity, workforce compliance, and risk monitoring to proactively safeguard customer trust, business resilience, and regulatory adherence.

5.5.3 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.

5.5.4 Cloud Infrastructure Risk Mitigation - Guidelines

The matrix below summarizes key risk management controls essential for mitigating cloud infrastructure risks and enhancing security posture.



5.5.5 Product Implementation Risk

Delays, errors, or omissions during project implementation can severely impact delivery commitments, particularly in a FinTech environment where clients rely on timely and accurate deployment of technology solutions. Such lapses may lead to delayed revenue recognition, missed billing milestones, and breaches of contractual service levels. This, in turn, can result in financial penalties, strained client relationships, and reputational harm to the brand. Additionally, repeated implementation issues may diminish client trust, affect reference ability, and pose challenges in securing future business, especially in regulated sectors where reliability and responsiveness are critical.

5.5.6 Product Implementation Risk Mitigation - Guidelines

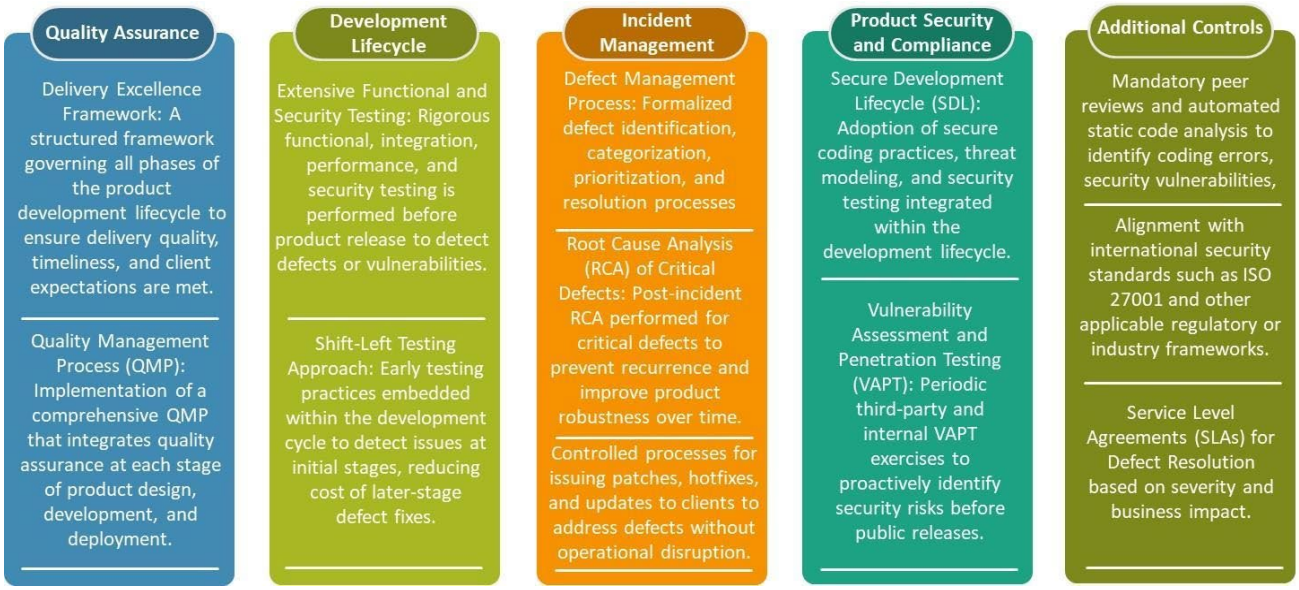
To address product implementation risk and ensure delivery reliability, below matrix consolidates multi-layered mitigation approach.

5.5.7 Defects & Security Vulnerabilities Risk

Failure to detect functional defects or security vulnerabilities in Intellect's products, whether during initial development or in subsequent updates and enhancements, poses a significant risk to product integrity and customer satisfaction. Products that do not meet client expectations in terms of performance, quality, or security may result in operational disruptions on the client side and lead to dissatisfaction. Inadequate or delayed resolution of such issues can further compound the impact, affecting long-term client relationships. Potential consequences include contractual penalties, termination of agreements, or demands for product replacement. This can adversely affect the brand's reputation and reduce the marketability and future demand for the affected product line.

5.5.8 Defects & Security Vulnerabilities Risk - Mitigation Guidelines

The matrix below summarizes key risk management controls for mitigating defects and security vulnerabilities, emphasizing proactive quality assurance, secure development practices, incident management, and compliance measures to reduce risk exposure and strengthen product integrity.



5.5.9 Compliance Risk

Inadequate adherence to, or non-compliance with, material laws and regulations applicable in countries where the company operates can pose significant legal, financial, and operational risks. These include corporate governance requirements, tax obligations, labour laws, data protection statutes, foreign exchange regulations, and sector-specific compliance mandates. Non-compliance may result in regulatory sanctions, fines, penalties, legal proceedings, or, in extreme cases, suspension or closure of operations in affected jurisdictions. This can directly impact the company's revenue streams, delay business expansion, and harm its reputation with regulators, clients, and investors.

In a multi-jurisdictional operating model, the complexity of navigating varied statutory frameworks increases the likelihood of inadvertent compliance breaches. This is further compounded by evolving legal landscapes, language barriers, and differing regulatory enforcement mechanisms across geographies.

5.5.10 Compliance Risk Mitigation – Guidelines

The matrix below summarizes key risk management controls for mitigating compliance risks, focusing on centralized compliance management, robust governance frameworks, ongoing statutory monitoring, and regular internal assurance to ensure regulatory adherence and operational integrity.

5.5.11 Litigation Risk

As Intellect operates across multiple jurisdictions, it is exposed to diverse and evolving regulatory, statutory, and legal frameworks. Each geography imposes its own set of legal obligations relating to commercial contracts, intellectual property rights, employment laws, data privacy, consumer protection, and financial regulations.

Engagement in legal proceedings, whether through regulatory actions, customer disputes, or third-party claims, presents inherent uncertainty. Such proceedings may lead to unfavourable outcomes, including monetary penalties, compensatory damages, injunctive relief, operational restrictions, or reputational harm. In extreme cases, adverse legal rulings may affect the company's ability to continue or expand its operations in certain regions, disrupt contractual relationships, or create barriers to new market entry.

Given the interconnected nature of global operations, legal exposure in one jurisdiction could also trigger regulatory scrutiny or reputational risks in others. Prolonged litigation, even where successfully defended, can be resource-intensive, divert management attention, and result in financial and operational strain.

5.5.12 Litigation Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for mitigating litigation risk, emphasizing proactive contract governance, structured management oversight, ongoing legal monitoring, and additional controls such as legal risk assessments and frontline training to minimize exposure and ensure effective dispute resolution.

5.5.13 Business Continuity Risk

In the current global landscape, shaped by escalating geopolitical tensions, evolving cyber threats, and increasing climate-related disruptions, the ability to sustain uninterrupted operations is a critical differentiator for organizations.

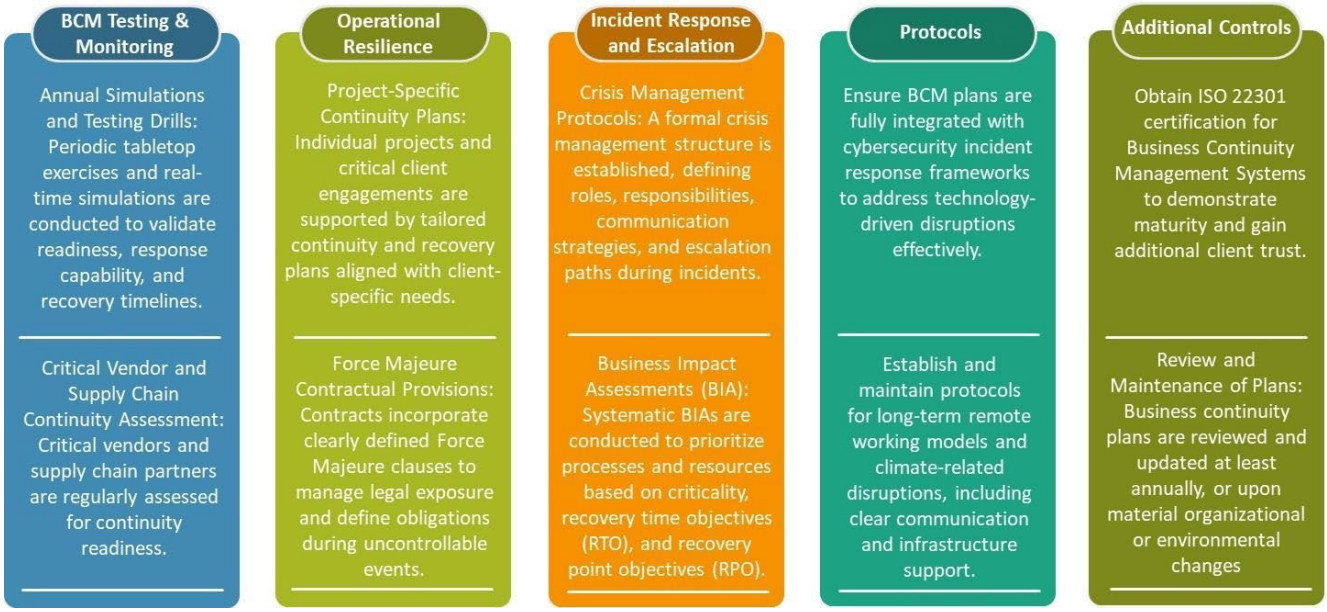
Inadequate or fragmented Business Continuity Plans (BCPs), particularly those that fail to comprehensively address people, processes, technology, and third-party dependencies, can significantly weaken an organization's resilience in the face of unforeseen events. These may include natural disasters, public health crises, cyberattacks, political unrest, supply chain breakdowns, or other Force Majeure scenarios.

Such disruptions can result in prolonged operational downtime, unmet client obligations, revenue loss, reputational damage, heightened regulatory scrutiny, and diminished stakeholder confidence. The complexity of global operations further amplifies these risks, as localized events may trigger systemic impacts across interconnected service delivery networks.

A robust, adaptive, and regularly tested Business Continuity Management (BCM) framework is essential to mitigate these risks. This includes clear detailing on cloud infrastructure, ensuring the availability of both primary and secondary servers across diverse geographic locations to maintain operational continuity and safeguard against localized outages. An effective BCM approach underpins client trust, ensures regulatory compliance, protects employee welfare, and preserves competitive advantage in volatile environments.

5.5.14 Business Continuity Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for business continuity, providing a structured approach to proactively identify, assess, and mitigate operational risks, ensuring organizational resilience and uninterrupted service delivery during disruptive events.



5.5.15 Fraud Risk

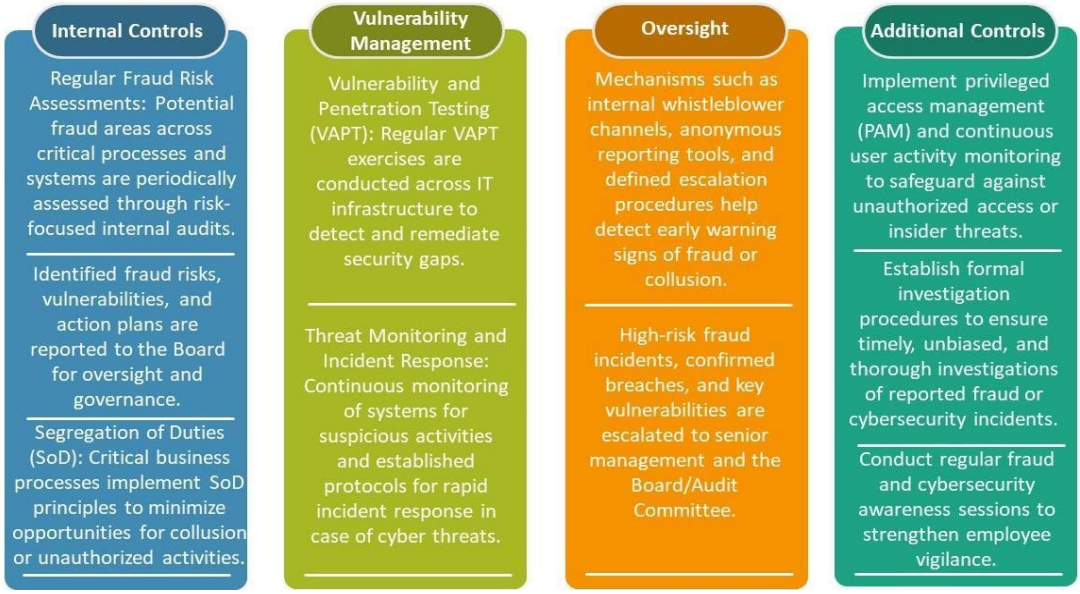
The risk of internal collusion, fraud, or external criminal hacking poses a serious threat to the company's financial stability, operational integrity, and reputation. If mechanisms to prevent, detect, monitor, and report potential fraudulent activities or cybersecurity breaches are inadequate or ineffective, the organization may suffer revenue leakage, direct financial losses, regulatory scrutiny, and erosion of stakeholder trust. Potential touchpoints for fraud include process loopholes, system vulnerabilities, weak access controls, inadequate segregation of duties, and human collusion. Additionally, cyberattacks such as hacking, phishing, or ransomware targeting products, financial systems, or client data can amplify the financial and reputational consequences.

Given the increasingly sophisticated nature of fraud and cyber threats, maintaining a strong, agile, and continuously evolving control environment is critical to ensuring early detection, timely response, and minimization of adverse impacts.

5.5.16 Fraud Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for mitigating fraud risk, highlighting proactive internal controls, continuous vulnerability management, robust

oversight mechanisms, and advanced detection and response measures to prevent, detect, and respond to fraudulent activities across the organization.



5.5.17 New Country Entry Risk

Failure to thoroughly study, evaluate, and address country-specific risks during expansion into new geographies can significantly compromise an organization's long-term strategic objectives, operational continuity, and brand reputation. Entering a new market requires navigating a complex set of political, economic, legal, regulatory, and sociocultural factors, each capable of materially affecting business outcomes if not properly assessed.

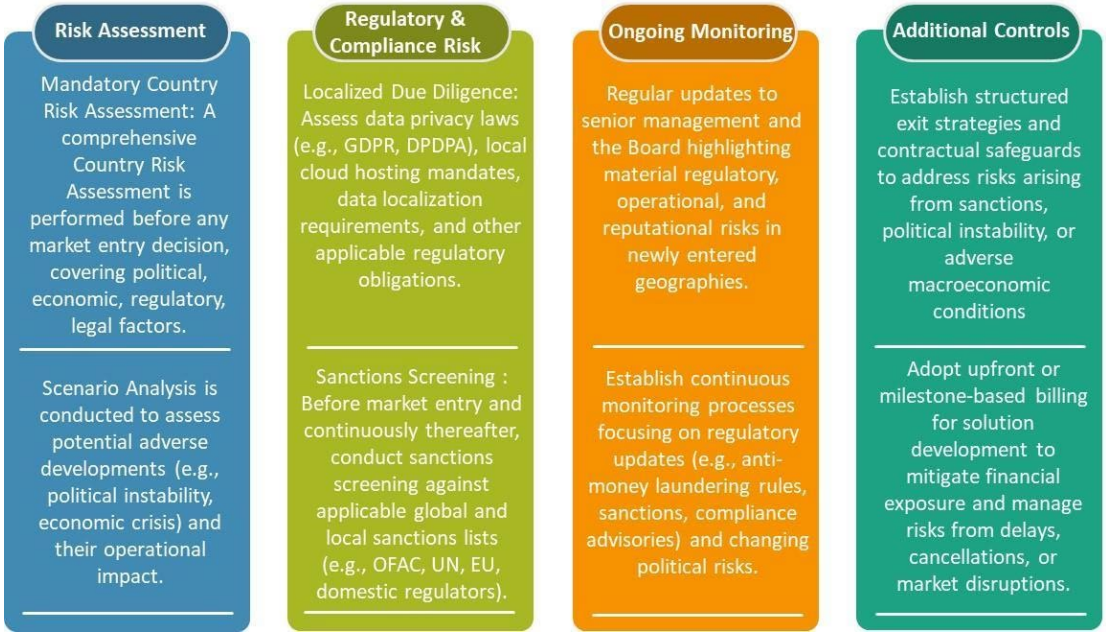
Without a formalized Country Risk Assessment, organizations expose themselves to critical uncertainties such as sudden regulatory changes, political instability, economic downturns, enforcement of protectionist policies, corruption risks, cultural mismatches, and social unrest. These risks could lead to operational disruptions, compliance violations, financial losses, reputational harm, or even forced exits from the market.

A Country Risk Assessment acts as an essential decision-making tool, enabling structured evaluation of external environmental factors before committing resources. It informs tailored business strategies, facilitates proactive regulatory alignment, fosters better local stakeholder engagement, and strengthens operational resilience. By embedding country risk analysis into strategic planning and enterprise risk management (ERM) frameworks, organizations position themselves for sustainable international growth while preserving governance standards and shareholder value.

5.5.18 New Country Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for new country entry, focusing

on comprehensive due diligence, regulatory and compliance assessment, ongoing risk monitoring, and additional safeguards to address political, economic, legal, social, and operational uncertainties associated with international expansion.



5.5.19 SUSTAINABILITY (ESG) RISK

Environmental, Social, and Governance (ESG) risks refer to the potential adverse effects on the organization's operations, financial performance, reputation, and regulatory standing arising from environmental, social, and governance factors. In the context of Intellect, environmental risks include the impact of operations on climate change, carbon emissions from data centres and cloud services, resource consumption, and vulnerabilities arising from environmental disruptions.

Social risks pertain to the organization’s influence on human rights, data privacy, financial inclusion, workforce diversity, community engagement, and ethical treatment of customers and employees.

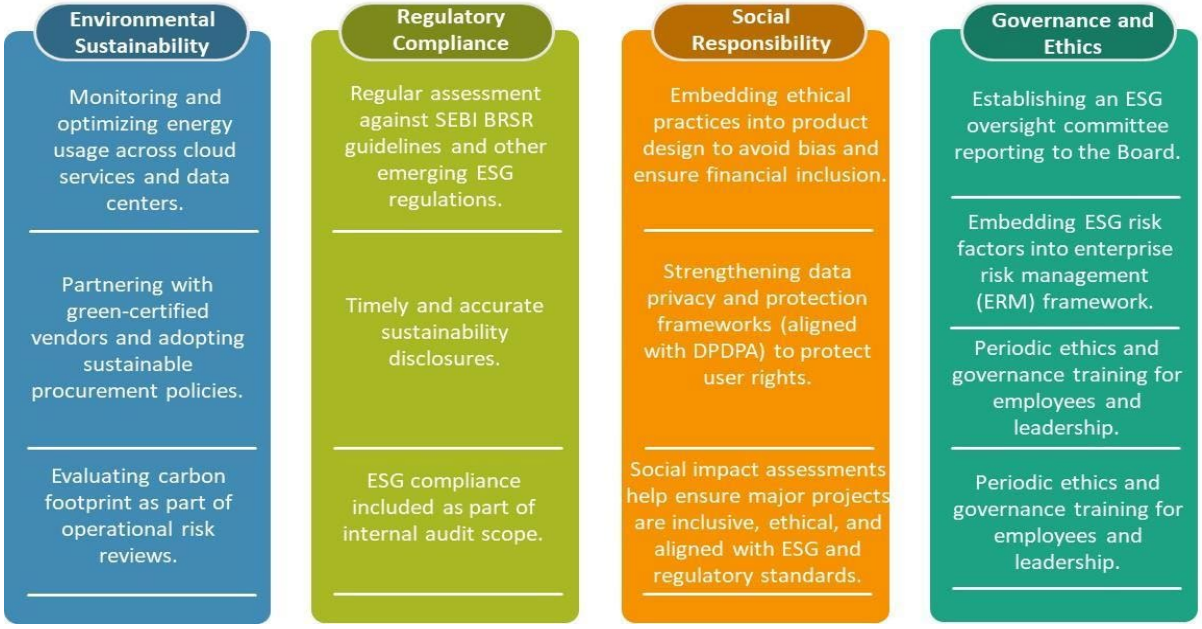
Governance risks arise from weaknesses in leadership oversight, transparency, accountability, ethical conduct, regulatory compliance, and the management of third-party and technology-related risks.

ESG risks may manifest through regulatory penalties for non-compliance with evolving disclosure standards (e.g., SEBI BRSR guidelines, IFSC mandates), reputational damage from perceived ethical lapses, operational disruptions due to environmental events, or loss of stakeholder confidence resulting from social or governance failures. Effective identification, assessment, and management of ESG risks are integral to maintaining the organization’s

operational resilience, legal compliance, stakeholder trust, market competitiveness, and long-term sustainability.

5.5.20 SUSTAINABILITY (ESG) RISK Mitigation - General Guidelines

The matrix below summarizes key risk management controls for mitigating sustainability risks, encompassing environmental, social, and governance (ESG) factors through comprehensive risk identification, stakeholder engagement, regulatory compliance, and continuous monitoring to ensure long-term organizational resilience and responsible business practices.



5.6 FINANCIAL CAPITAL

The Financial Capital component under the BEIELF framework focuses on safeguarding an organization's financial strength, stability, and reporting integrity. For a FinTech firm, this encompasses managing risks related to revenue sustainability, investment planning, liquidity, capital adequacy, and accurate financial disclosures. It includes mitigating risks from volatile market conditions, regulatory fines, credit exposures, and operational disruptions that could materially impact financial performance.

Sound financial capital management ensures the organization can meet its strategic growth objectives, comply with regulatory requirements, maintain investor confidence, and withstand financial shocks in a highly dynamic FinTech environment.

5.6.1 Liquidity Risk

In a FinTech product-based business model, where customers are primarily large banks and financial institutions, the inherent risk of credit default is relatively low. However, the

complexity and duration of order-to-cash cycles introduce significant liquidity and working capital risks.

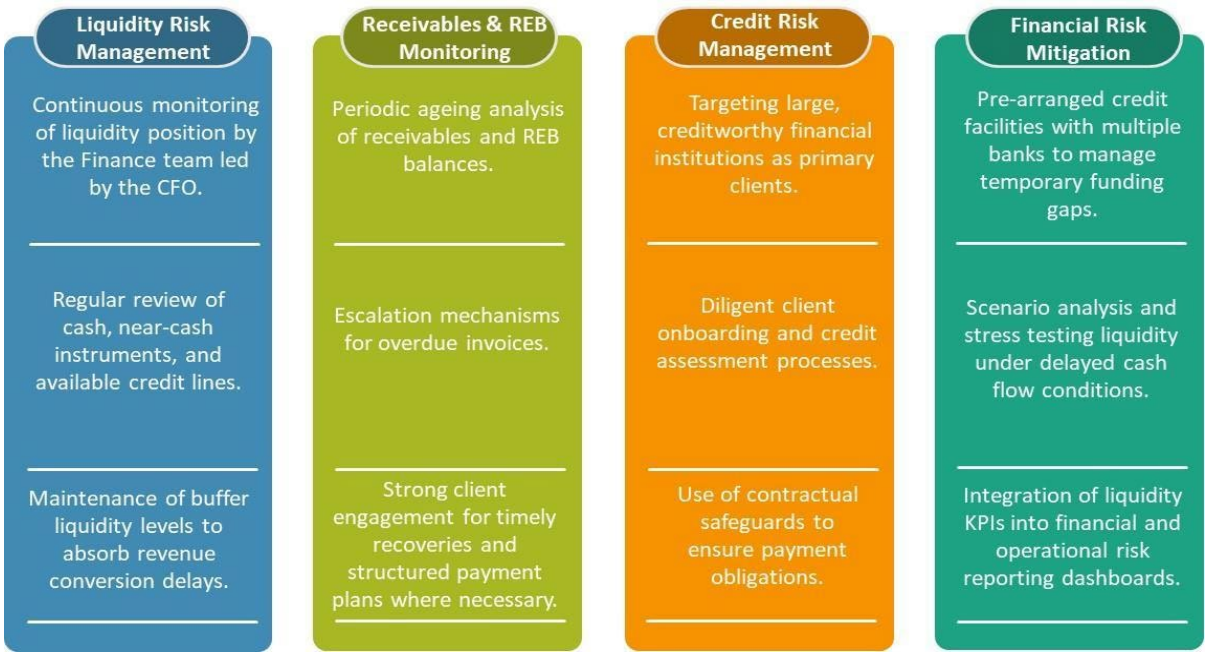
Delays in converting Revenue Earned but Not Billed (REB) into invoices, coupled with slow recovery of billed receivables, can strain the company's ability to meet critical operating expenses, such as salaries, vendor obligations, technology upkeep, and product development costs. Prolonged cash flow mismatches may increase reliance on short-term external funding, resulting in elevated finance costs, reduced profitability, and diminished financial flexibility. In the context of Intellect, such delays also constrain strategic investments in innovation and growth, undermining competitiveness and long-term resilience.

To mitigate liquidity risk, the company maintains access to non-debt-based financing instruments such as bank guarantees and sanctioned credit lines, ensuring flexibility without incurring long-term debt liabilities. These instruments serve as important buffers during periods of receivable stress, allowing operations to continue without disruption.

Liquidity risk remains a material area of focus, necessitating continuous monitoring and agile financial planning to sustain operations, support growth initiatives, and uphold financial stability.

5.6.2 Liquidity Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for liquidity risk, covering all critical pillars, risk identification, measurement, monitoring, and mitigation—to ensure sufficient liquidity, diversified funding, robust scenario testing, and effective contingency planning for uninterrupted financial operations.



5.6.3 Market Risk

In the FinTech sector, where revenue streams are often global and denominated in foreign currencies, market risk arising from foreign exchange (FX) volatility is a material concern. For Intellect, a significant portion of revenue is earned in foreign currencies, while a considerable part of expenses, particularly employee costs, infrastructure, and local operations, are denominated in Indian Rupees or other local currencies. Unhedged FX exposure can lead to unrealized losses, cash flow mismatches, and volatility in reported earnings, especially when currency movements are abrupt or sustained over a period. This can impair financial predictability, affect profitability, and potentially lead to investor uncertainty. In a FinTech model with long project cycles and milestone-linked billing, even minor fluctuations can materially impact margins if not properly managed.

Hence, currency risk management is critical to maintain financial stability, protect shareholder value, and ensure reliable cash flow planning.

5.6.4 Market Risk Mitigation - General Guidelines

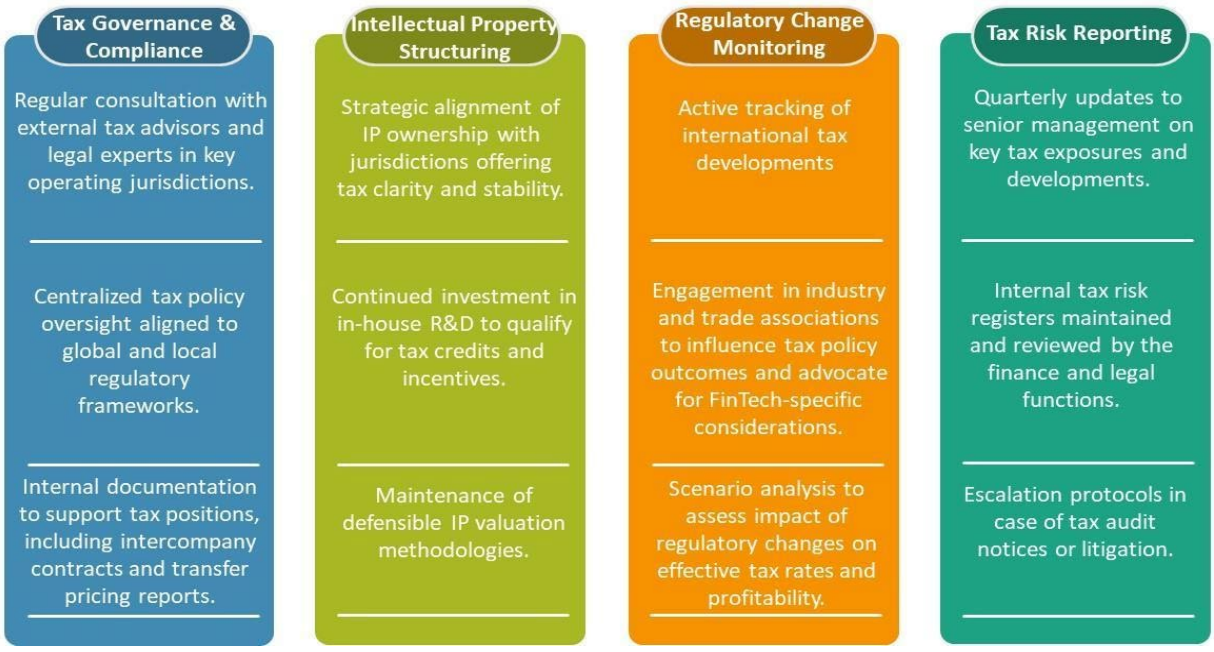
The matrix below summarizes key market risk management controls, providing a structured approach to identify, monitor, and mitigate risks arising from currency exposure, investment activities, treasury oversight, and audit processes to ensure financial stability and regulatory compliance.

5.6.5 Global Tax Regimes

As Intellect is operating across multiple jurisdictions, it is exposed to complex and evolving tax regulations, especially in areas related to intellectual property (IP), transfer pricing, and cross-border transactions. The IP-centric nature of its product business, combined with global client servicing, increases scrutiny from tax authorities over how revenue is attributed, IP is located, and intercompany pricing is determined. Amendments to tax regimes, such as digital services taxes, OECD BEPS 2.0 (Base Erosion and Profit Shifting), or changes to R&D-linked tax incentives, may increase compliance requirements, reduce eligible deductions, or create uncertainty in tax positions. This may lead to disallowances, tax litigation, penalties, and reputational risk, ultimately affecting profitability and financial planning.

5.6.6 Global Tax Regimes Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for global tax regimes, encompassing comprehensive tax governance, regulatory monitoring, intellectual property structuring, and robust reporting mechanisms to navigate complex international tax landscapes and ensure compliance across multiple jurisdictions.



5.6.7 Financial Reporting Risk

Intellect is required to comply with Section 134 of the Companies Act, 2013, which mandates the inclusion of a statement on Internal Financial Controls (IFC) in the Directors' Report, and an evaluation of their adequacy by statutory auditors. For FinTech firms, handling complex financial transactions, SaaS-based revenue models, and global operations,

ineffective or weak IFC frameworks pose significant risks. If internal controls over financial reporting are not adequately designed, implemented, or monitored, this may lead to misstatements, misclassification of revenue or costs, and errors in regulatory disclosures. These issues can compromise the true and fair view of financial results, lead to audit qualifications, expose the firm to regulatory penalties, and weaken investor confidence.

The specific risks include revenue recognition errors, weak system access controls, lack of audit trails in cloud environments, or insufficient validation of platform-based financial data, all of which can impact the integrity of financial reporting and compliance.

5.6.8 Financial Reporting Risk Mitigation - General Guidelines

The matrix below summarizes key risk management controls for financial reporting risk, encompassing regulatory compliance, robust control design and effectiveness testing, technology-enabled financial controls, and ongoing monitoring and reporting to ensure accuracy, transparency, and integrity in financial disclosures across the organization.

6 Cross-Functional Risk Collaboration and Oversight

As part of its mandate to ensure effective risk governance and integration across the organization, the Risk Management team shall engage with Business and Operations functions on a periodic and structured basis. These interactions are essential to support the consistent application of the risk management process and to strengthen the first line of defence.

Objectives of Engagements

a. Risk Identification and Mitigation Review

- Facilitate structured risk identification workshops to assess current risks and validate mitigation controls.
- Capture and review emerging risks through dynamic assessments based on changing internal and external conditions.

b. Review of Policies, Processes, and Controls

- Assess alignment of business processes and internal controls with defined risk frameworks.
- Provide feedback on policy adequacy from a risk perspective to ensure consistency, transparency, and control effectiveness.

c. Evaluation of Strategic and Operational Decisions

- Engage in the review of key decisions or strategic initiatives with potential material impact.
- Conduct forward-looking risk analysis to assess implications on solvency, profitability, and strategic alignment.
- Collaborate with relevant functions per the established SOP.

d. KRI Monitoring and Escalation Protocols

- Work with functional leaders to identify department-specific key risks and define appropriate Key Risk Indicators (KRIs).
- Establish and monitor practical threshold limits and escalation triggers for KRIs through consensus with business stakeholders, ensuring proactive risk response aligned to operational resilience goals.

e. Building Risk Ownership and Awareness

- Drive awareness of enterprise risk principles and risk processes.
- Reinforce the role of the first line of defence in identifying, escalating, and managing risks within their domain.
- Promote a proactive risk culture through training and cross-functional sessions.

7 Risk Management Approach

The Company's Risk Management Approach is a structured, proactive, and continuous process designed to identify, assess, prioritize, mitigate, and monitor risks that may impact the organization's strategic objectives, financial stability, regulatory compliance, and operational resilience. This approach is grounded in leading risk management practices and aligned with the Company's risk appetite, business model, and external environment.

It consists of the following 5 core steps:

a) Risk Identification

Identifying risks is the foundational step of the risk management process. The Company regularly assesses both internal and external environments to determine potential threats that could result in financial loss, reputational damage, legal liability, or regulatory breaches.

Risk identification is informed through various inputs, including:

- Periodic Risk and Control Self-Assessments (RCSA)
- Strategic or operational changes
- Industry trends and regulatory developments
- Internal and external fraud incidents
- Historical loss data analysis
- Outsourced activity assessments

b) Risk Evaluation

Once identified, each risk is evaluated to understand its likelihood of occurrence and potential impact on the organization, considering the size, complexity, and market dynamics in which the Company operates. Risks are rated as High, Medium, or Low in line with the Company's Risk Rating Guidelines.

c) Risk Prioritization

Risks are then prioritized based on their severity and alignment with the Company's defined Risk Appetite. Risk Appetite represents the level and type of risk the Company is willing to accept in pursuit of its strategic and operational goals. Functional units define specific risk tolerance thresholds, enabling informed decision-making. The Risk Management team facilitates risk appetite articulation, monitors exposure against tolerance levels, and escalates risks exceeding thresholds for mitigation or executive review.

d) Risk Mitigation

For risks identified as exceeding acceptable thresholds, appropriate mitigation strategies are developed. These may include risk avoidance, transfer, reduction through controls, or acceptance with monitoring. Action plans are designed by respective risk owners and monitored by the Risk Management function for effectiveness.

e) Risk Monitoring and Review

The Company continuously monitors its risk environment and the effectiveness of mitigation measures through regular reporting to senior management and relevant Board Committees. The monitoring framework includes:

- Scorecard-Based Risk Metrics (aligned to L0/L1 framework)
- Control Effectiveness Insights from Functional Scorecards
- Scenario Response Evaluation Reports
- Third-Party Risk Assessment Outcomes
- Business Continuity Validation Results

This structured approach enables early risk detection, supports compliance with regulatory expectations, and ensures informed, risk-based decision-making across the organization.

7.1 Principle-Based Risk Oversight Framework

In alignment with the dynamic nature of the Fintech sector, the Company focuses on a principle-based approach to risk oversight in lieu of traditional, static risk appetite statements. This framework ensures structured, responsive, and auditable risk governance, while aligning with evolving regulatory expectations (e.g., RBI, SEBI, IFSCA, DPDPA) and the Company's operational model.

7.1.1 Embedded Risk Governance

- The **Risk Management Committee (RMC)** conducts **half yearly reviews** of top enterprise risks, including data governance, cybersecurity, vendor dependency, data breaches, and technology failures.
- **Strategic initiatives** such as new module launches, cross-border partnerships, or on boarding of material vendors will be reviewed through a fit-for-purpose risk evaluation process. This will include basic regulatory and reputational checks, informal consultations with relevant stakeholders (e.g., legal, compliance, risk), and the use of simple checklists or documented observations to flag any red flags, such as sanctions risks, customer impact, or data exposure concerns, prior to final approval.

7.1.2 Real-Time Control Environment

- **Risk mitigation** will be embedded into day-to-day operational workflows through automation and business rule logic, enabling proactive identification and response to risk events.
    - For example, trigger-based detection can automatically flag or block unusual transactions based on behaviour patterns and set thresholds.
- **Risk Control Self-Assessment (RCSA)** is conducted annually to map key processes to inherent risks, control ownership, and mitigation status.

7.1.3 Operational Capacity and Resilience Thresholds

- Well defined **operational resilience thresholds**, including:
    - **Service uptime SLA** for customer-facing systems.

- **Maximum acceptable outage duration** for core platforms.
- **Customer dispute resolution TAT**

- **Quarterly stress simulations** (e.g., FinTech-specific events such as API downtime, payment gateway failure) will be run to validate contingency preparedness.

7.1.4 Product and Feature Risk Review

- All major product rollouts or changes must complete a risk and compliance readiness assessment, including security and privacy controls mandated under the integrated assurance framework.
- Pre-agreed exit criteria, such as disabling a feature of observed losses, fraud incidents, or regulatory concerns cross an acceptable threshold relative to transaction volume or customer impact.

7.1.5 Regulatory Compliance as De Facto Threshold

- In the absence of internal limits, **external regulations will serve as implicit risk boundaries**:
  - **DPDPA** for consent, data retention, and breach notification.
  - **RBI guidelines** for cyber hygiene (especially if offering APIs, wallets, or interfacing with banks/NBFCs).
  - **FATF and AML norms** if enabling any form of fund flow, even indirectly.

7.1.6 Culture of Risk Awareness and Escalation

- Periodic dashboards will be published to track key risk indicators relevant to platform stability and customer experience. These may include system uptime, on boarding drop-offs indicating KYC or fraud friction, volume and severity of customer complaints, and incidents involving unauthorized access.
- For high-severity events such as extended platform outages or coordinated fraud incidents, a cross-functional response team will be activated to manage resolution and communication.

7.2 Risk Management Tools / Methodology:

The Company has established a practical and structured risk management framework tailored to its operating model. This framework integrates risk oversight into key business functions such as product delivery, compliance, cybersecurity, vendor governance, and business continuity. Risk identification, monitoring, and mitigation are driven through a combination of self-assessments, key risk indicators, targeted reviews, and incident management protocols. The approach emphasizes regulatory alignment, operational resilience, and continuous stakeholder engagement, with regular reporting to the Risk Management Committee of the Board.

7.2.1 Risk Assessment and Oversight Summary

Periodic enterprise-wide risk assessments anchored in scorecard metrics and the Company's L0/L1 process framework, are presented to the Risk Management Committee (RMC) of the Board. These assessments offer a structured view of the Company's evolving risk landscape and include:

- **Scorecard-Based Control and Risk Insights -** Synthesized view of functional and enterprise-level risk signals using standardized evaluation metrics across business units.
- **Operational Threshold Monitoring -** Identification of emerging risk trends and deviations from defined performance or control thresholds, with recommended actions for course correction.
- **Summary of Material Risk Observations -** Highlights of significant exposures, unresolved issues, and management responses to mitigate residual risk and preserve business continuity.

7.2.2 Capital Assessment for future uncertain events

The Company conducts forward-looking capital planning through its annual business planning exercise. While it does not operate under regulatory capital requirements like banks or NBFCs, it evaluates financial buffers and operational flexibility against the following variables:

- Fluctuations in business volumes and client mix
- Shifts in product and delivery models
- Currency exposure and cost variations
- Changes in productivity and margin structures

This helps define sustainable growth objectives while preserving financial resilience. Cash flow and solvency positions are periodically reviewed and reported to the Audit Committee.

7.2.3 Profitability Analysis

The Company shall conduct periodic analysis of the product profitability and evaluate 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.

7.2.4 Control Self-assessment

Each business unit performs periodic self-assessment to identify key risks, control effectiveness, and gaps using a Risk Assessment Matrix. This exercise documents:

- Gross risks and control points
- Residual exposures not fully mitigated
- Action plans with defined ownership

The overall risk profile and movement across functions are reviewed by the RMC.

7.2.5 Functional Risk Reviews

Targeted deep-dive reviews are conducted on critical functions based on the approved Risk Management Plan. The focus is on practical control design, process vulnerabilities, and emerging risks. Review outcomes are discussed with business heads and summarized for the Risk Management Committee (RMC).

7.2.6 Enterprise Key Risk Indicators

The Company monitors enterprise-level and functional KRIs to track material risk exposures in real time. Examples include platform uptime, client complaints, fraud attempts, and delivery risks.

- KRIs are rated Red, Amber, or Green based on defined thresholds
- Tolerance levels are reviewed in light of strategic shifts
- KRI status and trends are presented to the RMC on a regular basis

7.2.7 Customer Complaints redressal

A defined grievance redressal framework is in place with roles, escalation paths, and response timelines. The framework is monitored for service-level compliance and periodically reviewed to enhance customer experience.

7.2.8 Vendor Risk Management

The Company shall maintain a defined process for vendor due diligence prior to on boarding and registration. Information security requirements shall be assessed and enforced at all stages of the vendor lifecycle, particularly for those with access to or handling of the Company's systems or data. Risks arising from third-party involvement in business processes shall be identified, and appropriate controls shall be implemented before engagement, during the course of engagement, and at the time of renewal or termination.

7.2.9 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 Bribery guidelines etc. Associates are imparted trainings to build 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 of compliance shall be drafted / signed off by the Compliance department of the company.

Sales Compliance: The Company shall establish a 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 miss-selling. This shall be achieved through regular business review meetings, quality reviews, self-assessments and compliances.

Project Implementation / Delivery Excellence Framework: The Company shall follow the Delivery Excellence framework wherein the 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 analyse and prioritize risks based on impact and probability of occurrence and identify suitable mitigation measures or contingency plans. 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.

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.

7.2.10 Information and Cybersecurity

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

- Provide direction and support for information & cyber security;
- Facilitate to establish the governance framework on Information Security Management System (ISMS) Standards and Procedures to protect the Company's information assets;
- Provide guidance for standards to protect information, computer systems and networks from threats and vulnerabilities from internal and/or external sources;
- 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.

7.2.11 Business Continuity Plan

The Company is committed to provide uninterrupted services to its customers 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.

7.2.12 Insurance

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

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

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

7.2.13 Risk Awareness

Building risk awareness is a core element of the Company's governance model. Periodic sessions and communications are conducted across functions to promote understanding and reinforce the importance of risk management. These include:

- Employee roles and responsibilities in managing risks
- Key internal and regulatory guidelines
- Controls and actions to mitigate department-specific risks.

8 Glossary

Term	Definition/Meaning
Enterprise Risk Management (ERM)	A structured process for identifying, assessing, prioritizing, mitigating, and monitoring risks across an organization to achieve strategic objectives.
Risk Identification	The process of recognizing and documenting potential risks that could affect the organization's objectives.
Risk Assessment	Evaluating the likelihood and impact of identified risks using qualitative or quantitative methods to prioritize them.
Risk Mitigation	Developing strategies to reduce the likelihood or impact of risks; includes risk reduction, transfer, acceptance, and avoidance.
Risk Monitoring & Control	Ongoing tracking of identified risks, monitoring risk triggers, and evaluating the effectiveness of mitigation actions.
Internal Controls	Processes, policies, and procedures designed to ensure the integrity of financial and operational information, promote accountability, and prevent fraud.
Communication & Stakeholder Engagement	Regular and transparent sharing of risk information with stakeholders to support informed decision-making.
Lessons Learnt	Capturing and analyzing past risk events to improve future risk management strategies.

Continuous Improvement	Regularly updating risk management processes and tools to enhance effectiveness and adapt to changing conditions.
Three Layers of Defence	A risk management model with three levels: 1) Operational management, 2) Risk management and compliance, 3) Internal audit—each with distinct roles in risk oversight.
Risk Governance Structure	The organizational framework for managing risk, including roles, responsibilities, and accountability at all levels.
BELIEF Framework	A risk management model (Brand, End Customer, Leadership, Intellectual Property, Execution, Finance) tailored for Intellect's FinTech operations, ensuring holistic risk coverage.
Brand Risk	The potential for loss due to damage to the company's reputation or market perception.
Reputational Risk	Risk arising from negative publicity, operational failures, or breaches that could harm the company's standing with stakeholders.
End Customer Risk	Risk of failing to meet the needs or expectations of clients (banks, financial institutions, etc.), leading to revenue loss or business failure.
Business Risk	The risk of not achieving business objectives due to market changes, competition, or operational failures.
Competition Risk	Risk of losing market share or profitability due to actions by competitors or changes in the market environment.
Model Risk	Risk of failure in adapting business models, pricing, or strategies to industry changes, especially related to cloud and technology transitions.
Concentration Risk	Risk from over-reliance on a single client, market segment, technology, or geographic region.
Customer Service Management Risk	Risks related to compliance, operational alignment, and relationship sustainability in client contracts across jurisdictions.
Contract Management Risk	Risk arising from non-performance or misalignment of contractual obligations with organizational capabilities or risk appetite.
Leadership Risk	Risk related to gaps in talent management, succession planning, or inappropriate conduct by associates.
People Risk	Risk from talent gaps, employee misconduct, or poor workforce management.
Intellectual Property (IP) Risk	Risk of loss, infringement, or unauthorized use of proprietary assets such as patents, trademarks, or software.
Information & Cyber Security Risk	Risk from cyber threats, data breaches, or IT system failures.
Data Protection &	Risk of non-compliance with data protection laws or mishandling of

Privacy Risk	personal/proprietary data.
Execution Risk	Risk that the organization fails to deliver on strategic objectives or client commitments due to operational failures.
Global Operational Risk	Risks arising from operating in multiple jurisdictions, including regulatory, legal, and geopolitical challenges.
Cloud Infrastructure Risk	Risk from non-compliance with SLAs, security breaches, or inadequate resources in cloud environments.
Product Implementation Risk	Risk of delays, errors, or omissions during project implementation, affecting delivery and client satisfaction.
Defects & Security Vulnerabilities Risk	Risk that product defects or security flaws cause operational disruptions or reputational harm.
Compliance Risk	Risk of failing to comply with laws, regulations, or internal policies, leading to legal or financial penalties.
Litigation Risk	Risk of legal disputes or regulatory actions that could result in financial loss or reputational damage.
Business Continuity Risk	Risk of operational disruption from events like disasters, cyberattacks, or supply chain failures, threatening service continuity.
Fraud Risk	Risk of financial loss or reputational damage from internal collusion, fraud, or external cyberattacks.
New Country Entry Risk	Risk from insufficient assessment of political, economic, legal, or cultural factors when expanding into new markets.
Sustainability (ESG) Risk	Risk from environmental, social, or governance factors that could impact operations, reputation, or regulatory standing.
Financial Capital Risk	Risk to the organization's financial strength, stability, and reporting integrity from market, credit, or operational disruptions.
Liquidity Risk	Risk that the organization cannot meet short-term financial obligations due to cash flow mismatches.
Market Risk	Risk from adverse movements in market prices, exchange rates, or interest rates.
Global Tax Regimes Risk	Risk from complex and evolving tax regulations in multiple jurisdictions.
Financial Reporting Risk	Risk of errors or misstatements in financial reports due to weak internal controls or system failures.
Cross-Functional Risk Collaboration	Collaboration between risk management and business functions to ensure consistent application of risk processes.
Key Risk Indicators (KRIs)	Metrics used to monitor and signal changes in risk exposure.

Risk Appetite	The level and type of risk an organization is willing to accept in pursuit of its objectives.
Control Self-Assessment (CSA)	A process where business units assess their own risks, controls, and gaps to improve risk management.
Vendor Risk Management	Processes for assessing and mitigating risks associated with third-party vendors.
Insurance	Coverage to mitigate financial losses from specific risks, such as cyber liability, errors and omissions, or property damage.