NEWGEN

RISK MANAGEMENT POLICY

Reference Number: Finance/ RMC – 2

Revision/Approval History			
Release Date	**Mode**	**Approved by**	**Approval date**
25-10-2021	Revised by Risk Management Committee	Board of Directors	25-10-2021

Contents

1. **OBJECTIVES:**

The Risk Management Policy intends to enable Newgen Software Technologies Limited ('NSTL' or the 'Company') to adopt a defined and documented framework for identifying and managing its risks regularly and to set out procedures to inform the Board of Directors of the Company about the risk assessment along with minimisation procedures. The Policy will give a structured and disciplined approach to Risk Management, including the development of the Enterprise Risk Register, and to guide the Company to make informed decisions on risk-related issues, which are important for sustained business.

2. **RISK MANAGEMENT PHILOSOPHY:**

Newgen's Risk Management Policy philosophy is to enable the achievement of the Company's strategic objectives by identifying, analysing, assessing, mitigating, monitoring, preventing, and governing any risks or potential threats to these objectives. The systematic and proactive identification of risks and mitigation thereof shall enable effective or quick decision-making, facilitate business continuity, and shall improve the performance of the organisation.

Risk Management at Newgen is a continuous process of analysing and managing the opportunities and threats faced by the Company to achieve its goals and ensure the continuity of the business, under industry best frameworks like ISO 31000, ISO 27001, etc.

3 **SCOPE:**

This is applicable to the Company, including its subsidiaries, and all processes or functions in such entities.

4 **RISK MANAGEMENT COMMITTEE:**

The Risk Management Policy ("Policy") will be implemented through the Risk Management Committee ("Committee") accountable to the Board of Directors and to the Audit Committee, wherever required.

The quorum necessary for transacting business at a meeting of the Committee shall be at least three members (including one Independent Directors) of the Risk Management Committee. The Committee may also invite other official(s) of the Company and its subsidiaries or consultant(s), as permitted by the Chairman of the Committee.

The role of the Committee shall, inter alia, include the following:

a) To formulate a detailed risk management policy and to recommend the same to the Board for its approval.
b) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.

c) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
d) To periodically review the risk management policy, at least once in two years, including considering the changing industry dynamics and evolving complexity.
e) To keep the Board of directors informed about the nature and content of its discussions, recommendation, and actions to be taken.
f) The Risk Management Committee shall have access to any internal information necessary to fulfil its oversight role. The risk management committee shall also have the authority to obtain advice and assistance from internal or external legal, accounting, or other advisors.
g) Review and recommend changes to the Risk Management Policy and/or associated frameworks, processes, and practices of the Company.
h) To constitute Internal Working Committee, as the necessary time to time to implement the Process related with Risk Management.
i) Perform other activities related to this Policy as requested by the Board of Directors or the Audit Committee or to address issues related to any significant subject within its term of reference or as may be prescribed by SEBI Regulations or Companies Act 2013, time to time.

5. RISK MANAGEMENT APPROACH:

The risk may be caused by Internal and External issues (i.e., Context to the organisation) or due to the occurrence of uncertain catastrophic acts (natural or man-made). These may impair the Company's assets, which may adversely influence the achievement of organisation strategies, operational & financial objectives, earning capacity & financial position. The Process of Risk Assessment shall cover the following:

a) Identification and Categorisation of Risks
b) Risk Assessment and Evaluation
c) Risk Response and Mitigation
d) Risk Monitoring and Reporting

5.1 IDENTIFICATION AND CATEGORISATION OF RISKS

'Internal and external issues relevant to Newgen business' and 'Expectations and needs of its interested parties (internal and external)' shall be considered for identifying the risks. This would envisage identifying the potential list of events / risks / factors that could have an adverse impact on the achievement of business objectives. Risks shall be identified through Business Impact Analysis ("BIA") under the following broad categories. This is an illustrative list and not necessarily an exhaustive classification.

S. No	Risk Categories	Risk Definitions
1.	Strategy risks	Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

2.	Financial risks	Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.
3.	Governance risks	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
4.	Operations risks	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
5.	Legal risks	Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
6.	Property risks	Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
7.	Commercial risks	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.
8.	People risks	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance
9.	Technology risks	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
10.	Information risks	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
11.	Security risks	Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and

		information, including cyber security and non-compliance with General Data Protection Regulation requirements.
12.	Project/Programme risks	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
13.	Reputational risks	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

a) Reporting and formatting of Business Impact Analysis ("BIA") shall be reviewed and approved by the Committee from time to time.

b) Risks shall be identified in the risk register by the relevant authorities.

5.2 RISK ASSESSMENT AND EVALUATION

The Committee shall formulate and established an SOP on Risk Assessment and Treatment Process, which shall also include the following: -

a) The risk assessment shall be undertaken half-yearly, as directed by the Risk Management Committee or as and when there is a change in the business circumstances. Some of the scenarios (*include but not limited to*) in which the Risk Assessment shall be initiated are
   - New or changed service(s)/asset
   - New infrastructure (location, floor, etc.)
   - New or changed asset (physical/software/information/service)
   - New or changed supplier relationship
   - Against the contractual requirements

b) Risks shall be assessed using two-fold criteria i.e.
   - Likelihood: the probability of risk occurrence
   - Impact: magnitude of the effect if the risk occurs

c) Likelihood (1-5) and Impact Value (1-5) shall be identified considering the current implemented controls in the organisation.

d) Rating and criteria for Likelihood and Impact are given in the Risk Management Process.

e) Combining Likelihood and Impact will give the Risk Index or suggest the level of risk to the organisation.

f) Basis the Likelihood and Impact the risk shall be prioritised as below

- High Priority: These are critical risks, require immediate action, and require monthly monitoring by the Risk Owner.
- Medium Priority – These are the risks with high likelihood/impact value and require monitoring quarterly by the Risk Owner.
- Low Priority – These are the risk with low Likelihood/Impact and require monitoring on a six-monthly basis by the Risk Owner. These risks can be accepted by the Risk Owner.

g) Risk Owner shall be identified against every risks.

h) Refer to Annexure A for more details on Risk Evaluation Matrix.

5.3 RISK RESPONSE AND MITIGATION

a) Risk Response or Treatment shall identify the controls required for the treatment of the risks.
b) The Risk Response or Treatment shall include any of the following options
   - Risk Acceptance
   - Risk Transfer
   - Risk Control
c) Risk Treatment Plan shall be prepared to document the information like the risk description, likelihood, impact, treatment option, risk owner, controls to treat the risks, status, etc.
d) Business Continuity Plan shall be reviewed to ensure it is in alignment with the Risk Treatment Plan. Risk Owners to ensure business or service continuity risks are identified in the Enterprise Risk Register.

A detailed process of risk treatment shall be documented in the Risk Assessment and Treatment Process.

5.4 RISK MONITORING AND REPORTING

a) At the organisation level risks and the effectiveness of the controls as part of the Risk Treatment Plan shall be reviewed and monitored by the Risk Management Committee (RMC).

b) The review by the RMC shall be done twice in a year or as to when required due to some change in the business or market circumstances.

6 RISK REGISTER:

The Committee should ensure the compilation of a Risk Register in the appropriate format. The Risk Register shall be placed before the Committee twice a year.

7 BUSINESS CONTINUITY PLAN:

A business continuity ("COB") plan is a document that outlines how a business will continue operating during an unplanned service disruption. This plan addresses the recovery of Company's critical business projects/processes/assets after an interruption.

An interruption can be defined as any incident man-made or natural, intentional or unintentional that affects normal operations. Interruptions can be classified into 3 categories:

1. Malfunction: Minor interruptions that affect hardware, software, or data files. They are usually quite narrow in scope, confined to smaller area and it is usually possible to recover quickly from them. e.g. UPS breakdown, Electricity breakdown, Server breakdown/crash, virus attack etc.

2. Disasters: - Interruption to entire or partial facility. They typically require the use of alternate/off-site processing facilities to recover operations. Facilities may be disrupted for a significant period of time. E.g. Due to Fire, Earthquake affecting a site, any other infrastructure breakdown, pandemic, terrorist attack or act of vandalism etc.

3. Catastrophe: - This is the most serious type of interruption. In a catastrophe, the facilities may have been destroyed. Alternate facilities are always needed to process data. It may be necessary to rebuild or establish new or permanent facilities. E.g. Major Natural Calamity (Like Earthquake, Flood affecting entire city), War.

COB Plan keeps the business operational during adverse conditions from the time the event is under control to the time the business is restored and fully operational. COB plan enables Newgen to survive an interruption and to re-establish and continue normal business operations. The purpose is to minimise the impact of an interruption to business operations. It focuses on continuing critical functions through any interruption. It includes framework plan and a series of sequenced steps that allow the organisation to accomplish critical functions and eventually complete resumption of all functions. Newgen Continuity of Business Plan defines the continuity of Newgen Product, Delivery Services and other supporting functions along with a framework for Engagement specific Strategy for specific customer.

To assure that critical operations can resume within a reasonable time frame, the goals of the COB plan are:

- Ensure safety of employees, vendors, and customers within Newgen premises
- Minimise the duration of an interruption to business operations and resume the work expeditiously
- Facilitate effective co-ordination of recovery tasks
- Reduce the complexity of the recovery effort
- Ensuring necessary infrastructure to tackle any interruption.
- Minimising potential economic/ business loss
- Decreasing potential exposures
- Reducing the probability of occurrence
- Reducing interruptions to operations
- Ensuring organisational stability

- Protecting the assets of Newgen and Customer.

COB plan also defines procedures for disaster recovery, required training and ongoing procedures to maintain the plan. Special attention and emphasis is given to an orderly recovery and resumption of the operations that concern the critical business of running the on-going projects / processes, including providing support to clients under ATS/AMC and Newgen managed cloud services.

The Committee shall approve and review the COB Plan time to time as required.

8 **DISCLAIMER CLAUSE:**

The Management cautions readers that the risks outlined above are not exhaustive and are for information purposes only. Readers are therefore requested to exercise their own judgment in assessing various risks associated with the Company.

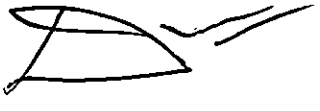
9 **POLICY REVIEW:**

This Policy should be reviewed once a year or earlier if required by a change in circumstances. The Board of Directors shall approve any modification on this Policy with the recommendation of the Committee.

10. **LIMITATION AND AMENDMENT:**

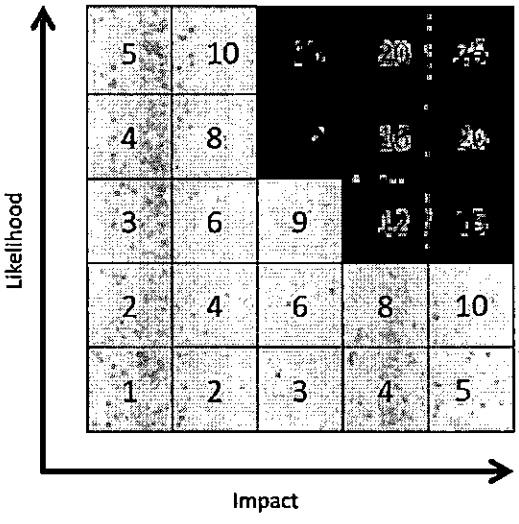
In the event of any conflict between the Act or the SEBI Regulations or any other statutory enactments ("Regulations") and the provisions of this Policy, the Regulations/ Act shall prevail over this Policy. Any subsequent amendment / modification in the Regulations, in this regard shall automatically apply to this Policy.

For **Newgen Software Technologies Limited**



Diwakar Nigam
Chairman & Managing Director

Annexure A - Risk Evaluation Matrix



Low Priority	Require monitoring at least on a six-monthly basis or as decided by the Risk Owner
Medium Priority	Require monitoring at least quarterly or as decided.
	Require immediate action and monthly monitoring

- Risks that shall have risk value in red zone, shall be considered as High Priority risks. Such risks must be treated immediately. Status of such risks shall be reviewed at least monthly by the Risk Owner.
- Risks that shall have risk value in the amber zone, shall be considered as Medium Priority. Status of such risks shall be reviewed at least quarterly by the Risk Owner.
- Risks that shall have risk value in the green zone, shall be considered as Low Priority. Such risks can be accepted; however, the status of such risks should be reviewed at least on a six-monthly basis by the Risk Owner.