NexTtech Limited

Risk Management Policy

A. Document Information:

Document Ref No.	: NEXTECH-ISMS-L2-003
Document Title	: Risk Management Policy
Revision No.	: 00
Issue Date	: 05 December 2020
Document Owner	: HoRisk
Prepared by	: Risk Dept., NEXTECH
Approved by	: CTO

B. Document Distribution List:

SN	Designation
1.	CTO
2.	HoRisk
3.	CISO
4.	Departmental Heads

Table of Contents

1. Introduction

Information security in NEXTECH assumes various risk from different stakeholders of the system. This Risk Management Policy guides the relevant personnel to assess information security risk and manage it appropriately.

1.1 Purpose

NEXTECH requires on-going Information Risk Assessment and Management. This procedure conforms to requirements of ISO 27001 standard that identifies threats and vulnerabilities, and results in a formal risk assessment. It can support other areas of risk assessment and management. The Objective of this policy can be listed as:

i) To identify risk areas and take preventive measures to minimize the loss to the organization;
ii) To protect businesses by keeping the company viable and reducing financial risks;
iii) To protect the physical facilities, data, records, and physical assets against attacks, theft, misappropriation, leakage, misuse etc;
iv) To have consistent processes, business and operational framework and standard operational procedures wherein everyone have common understanding on managing risks;
v) To provide guidelines to all NEXTECH employees on risk standards that shall be expected of risk management policy;
vi) To sets out the minimum risk identification, measurement, monitoring and control system that shall help all employees to understand the risk management policy.
vii) To provide guidelines in line with internationally accepted risk management principles and best practices.
viii) To protect the interest of shareholders and investors.

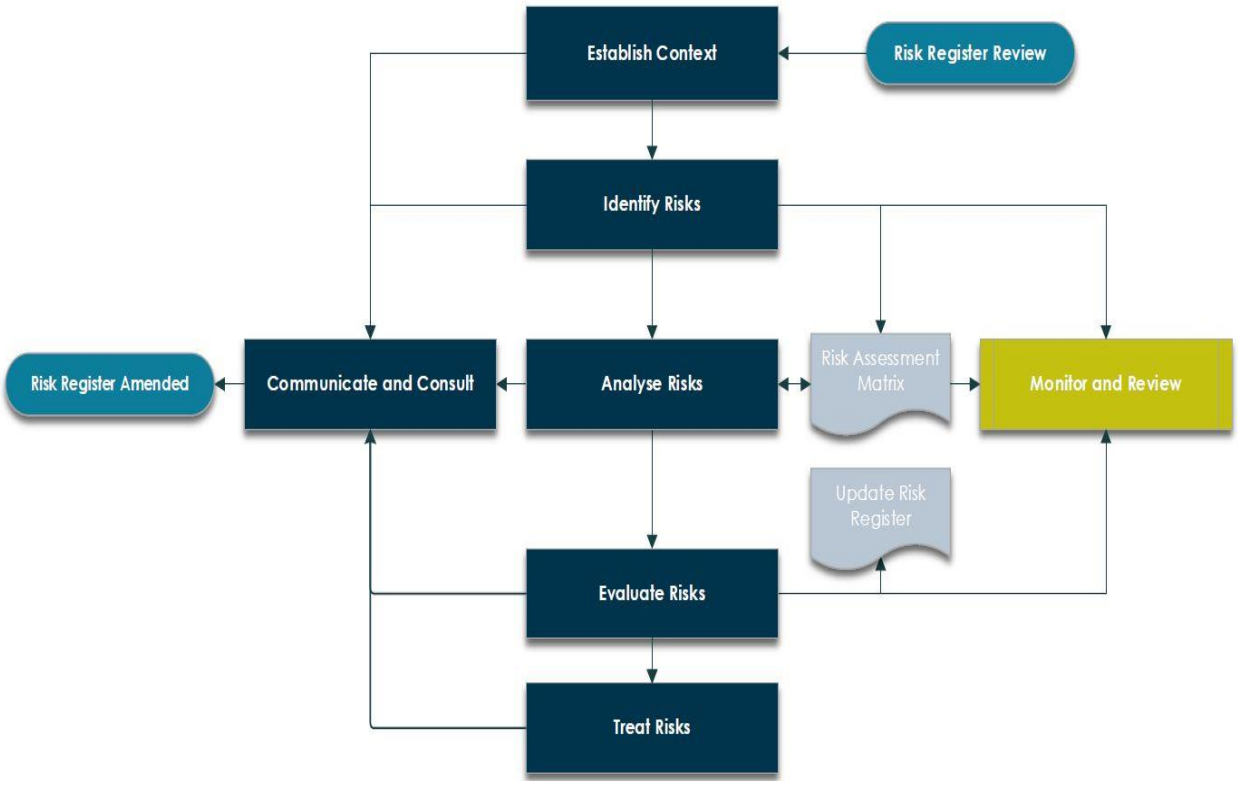
1.2 Scope

The risk management policy shall be regularly applied to all business processes and information assets within scope. It shall also be applied whenever there are significant changes that have an impact on the relevant scope e.g. changes to business processes, assets, technology, threats, vulnerabilities, and interfaces (e.g. IT network connections) and dependencies (e.g. third-party support)

2. Ownership and Responsibility

HoRisk

3. Workflow chart



4. Risk Management Policy

Risk is the possibility of an adverse event occurring with potential for negative implications. Risk management is the process of managing the likelihood or the severity of the adverse event to an acceptable range or within limits set by the organization.

A risk management policy is a guide for NEXTECH managers and organizational practice that helps them focus on the most important risks in an effective and efficient manner. The Risk framework is a consciously designed system to protect the organization from undesirable surprises (downside risks), and enable it to take advantage of opportunities (up-side risks).

4.1 Major Information Security Risks and Mitigation

Information security is always vulnerable to different risks. The risks is evolved from individuals involved within the process, the technology deployed to manage the information. Following factors are considered while identifying information security risks:

i) Risks from the innocent internal sources, arising from the negligence of the users during their usage of the system.
ii) Risks due to lack of awareness and knowledge of the users.
iii) Risk related to intentional internal sources, arising from the valid users who wants to sabotage within the organization.
iv) Risks from external sources like different types of malware, virus, fishing attacks coming over internet.

v) Unpredictable risks arising from disaster.

5. Risk Management Process

5.1 Establishing Context

Management of NEXTECH believe that before risk can be clearly understood and dealt with, it is important to understand the context in which it exists. Management should first define the relationship between NEXTECH and the environment that it operates in so that the boundaries for dealing with risk are clear. This step defines the overall environment in which a business operates and includes an understanding of the clients' or customers' perceptions of the business. An analysis of these factors will identify the strengths, weaknesses, opportunities and threats to the business in the external environment. Establish the content by considering:

- The strategic context – the environment within which the organization operates
- The organizational context – the objectives, core activities and operations.

5.2 Identify Risk

Risk cannot be managed unless it is first identified. Once the context of NEXTECH has been defined, the next step is to utilize the information to identify as many risks as possible. The aim of risk identification is to identify possible risks that may affect, either negatively or positively, the objectives of the business and the activity under analysis.

Key questions to ask include:

- What can happen?
- How and why it can happen? List the possible causes and scenarios or description of the risk, incident or accident.

Identification should include all risks, whether or not they are currently being managed. The rationale here is to record all significant risks and monitor or review the effectiveness of their control.

5.3 Analyze Risk

This involves analyzing the likelihood and consequences of each identified risk and deciding which risk factors will potentially have the greatest effect and should, therefore, receive priority with regard to how they will be managed. The level of risk is analyzed by combining estimates of likelihood and consequences, to determine the level of the risk.

The most important part of risk analysis is assessing and grading each and every risk identified. For each risk the Impact Assessment and its Likelihood Assessment should be done carefully. The risk grading should be done on a 5 point scale (Check the below tables).

Traffic Light	Assessment	Interpretation
Low	Rare, may occur in exceptional circumstances. No or little experience for a similar failure;	Less than 5%
Low/Medium	Might occur at some point in time. Conditions do exist for this to occur, but controls exist and are effective.	Between 5% and 10%
Medium	Could occur, this is possible. Measures to reduce likelihood exist, but may not be fully effective.	Between 10% and 20%
Medium/High	Will probably occur, measures may or may not exist to reduce likelihood.	Between 20% and 80%
High	Is expected to occur, almost certain.	Greater than 80%

Table-1: Likelihood Assessment

Grade of Impact	Description	Interpretation
Low	Fairly insignificant, may lead to a tolerable delay in the achievement of objectives or minor reduction in Quality/Quantity/ and/or an increase in cost.	No or minor financial implication.
Low/Medium	Some impact of the risk, fairly minor.	Minor financial implication, make the operation slightly difficult/complicated
Medium	Moderate effect. Risk factor may lead to delays or increase in cost.	Considerable impact for program with financial implications
Medium/High	Major effect. Risk factor may lead to significant delays or non-achievement of objectives.	Impact on country level objectives/ program. Financial implications.
High	May cause key objectives to fail. Very significant impact on organizational goals. Legal or regulatory implications. Significant reputational impact.	Significant impact on country and holding level, Significant impact on overall operation and financial implications high.

Table-2: Impact Assessment

IMPACT			Likelihood				
			Low	Low/Medium	Medium	Medium/High	High
			1	2	3	4	5
High	5		5	10	15	20	25
Medium/High	4		4	8	12	16	20
Medium	3		3	6	9	12	15
Low/Medium	2		2	4	6	8	10
Low	1		1	2	3	4	5

Low	1-6
Medium	7-12
High	13-25

Table-3: Risk Matrix

5.4 Treat Risk

Risk treatment involves identifying the range of options for treating the risk, evaluating those options, preparing the risk treatment plans and implementing those plans. It is about considering the options for treatment and selecting the most appropriate method to achieve the desired outcome. According to NEXTECH, treatment options include:

- **Transfer:** For some risks, the best response may be to transfer them. This might be done by conventional insurance or by supporting a third party to take the risk in another way.
- **Tolerate:** The ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. This course of action is common for large external risks. In these cases the response may be toleration but the risk should be tracked so managers are ready to reconsider should it start to escalate. Tolerance levels determining how much risk can be taken at each level need to be set and should inform your decisions.
- **Treat:** The purpose of taking action to reduce the chance of the risk occurring is not necessarily to obviate the risk, but to contain it to an acceptable level. Risk will be passed up and down the corporate chain. High-level risks may have to pass to a higher level of responsibility to decide on an action, whereas other risks may translate into activities designed to mitigate them. Decide what criteria will result in the risk being passed up the corporate management system.
- **Terminate** the risk by doing things differently thus removing the risk where it is feasible to do so.

5.5 Monitor and Review Risk

As with communication and consultation, monitoring and review is an ongoing part of risk management that is integral to every step of the process. It is also the part of risk management and given adequate focus to be effective. Monitoring and review ensure that the important information generated by the risk management process is captured, used and maintained.

Few risks remain static. Factors that may affect the likelihood and consequences of an outcome may change, as many the factors that affect the suitability or cost of the various treatment options. Risk management should be fully incorporated into the operational and management processes at every level of the organization and should be driven from the top down. The monitoring and review is usually should done by third line and second line of defense and in some cases by first line and reported to the second line.

5.6 Risk Management Tools

NEXTECH uses Risk Register, Risk Appetite and Risk Control Matrix to manage risk.

5.6.1 Risk Register

A risk register (NEXTECH-ISMS-F003) is maintained by NEXTECH. The risks are identified based on the guideline provided in this policy. This risk register is reviewed and updated every quarter. The risk register is provided in Annex I.

5.6.2 Risk Appetite

Risk appetite is defined as the amount of risk the organization is prepared to accept, tolerate, or be exposed to at any point in time. The Management has produced a risk appetite to provide direction on risk appetite and set the boundaries for risk management in NEXTECH. This provides clear guidelines to staff to indicate where risks can be taken and where they cannot.

- NEXTECH's Information Security risk appetite is set at a level to avoid losses
- NEXTECH has stated a separate risk appetite statement for each category of Information Security risk.
- NEXTECH will set specific tolerance level for each category of risk in January 2020 if deemed necessary
- NEXTECH will not compromise reputation from unethical, illegal and unprofessional conduct; and
- NEXTECH also maintains zero appetite for association with disreputable individuals

Information Security risk appetite for the listed risks is available in Annex II. This table is reviewed and updated every quarter.

5.6.3 Risk Control Matrix

The Risk Control Matrix records details of all the risks identified at the beginning and during operation, their grading in terms of likelihood of occurring and seriousness of impact on the project, identify controls in place, initial plans for mitigating each high level risk, the costs and responsibilities of the prescribed mitigation strategies and subsequent results. This table is reviewed and updated every quarter. Risk Control Matrix for the listed risks is available in Annex III.

6. Roles and Responsibilities

6.1 General Roles

Not applicable

6.2 Specific Roles and Responsibilities

5.2.1 Role: CISO

Responsibility
1. Implementation of the policy. 2. Ensure that policy is maintained and controls are effectively implemented. 3. Reviewing the policy for adequacy and completeness. 4. Managing conformity and taking action against any non-conformity. 5. Reporting to Top Management.

5.2.2 Role: HoRisk

Responsibility
1. Ensure that policy is maintained and controls are effectively implemented. 2. Reviewing the policy for adequacy and completeness. 3. Managing conformity and taking action against any non-conformity.

5.2.3 Role: CTO

Responsibility
1. Approving the policy. 2. Periodical review to identify relevance and applicability of change in the policy. 3. Provide all technical & Administrative support to HoRisk and CISO

5.2.4 Role: Management Committee

Responsibility
1. Providing support for effective implementation of the policy. 2. Periodical review of performance of the policy and providing resources as necessary. 3. Proving leadership.