Besseggen Risk Management Policy

Doc: Version: 1.2

Document Classification: Internal

Document Control

Document Name	Besseggen Risk Management Policy
Abstract	This document describes the Risk Management policy at Besseggen Infotech LLP.
Security Classification	Internal
Location	SECTOR-94, NOIDA, GAUTAM BUDH NAGAR-201301

Authorization		
Document Owner	Reviewed by	Authorised by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	Modification Date	Section	A/M/D	Brief description of change
1.1	18 APR 2022	ALL	A	Final
1.2	19 OCT 2023	10	M	Risk assessment reviewed

Distribution list
Chief Information Security Officer (CISO)

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Auditors (Internal & External)
All users,committee at Besseggen Infotech LLP.

TABLE OF CONTENTS

1. Overview

BESSEGGEN INFOTECH LLP (henceforth named as "BESSEGGEN") understanding its context and the needs & expectations of interested parties, shall determine the risks and opportunities that need to be addressed to ensure

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

the information security management system can achieve its intended outcome.

2. Objectives

To prevent, or reduce, undesired effects of risks and opportunities and evaluate the effectiveness of the actions taken and desired requirements.

- BESSEGGEN shall ensure that risks are identified and managed in an effective, efficient and timely manner considering their relevant impact on BESSEGGEN business.
- Risks shall be assessed and managed as part of all BESSEGGEN relevant activities (e.g., business functions, day-to-day operations, systems acquisition, development and implementation, systems operations and others), by ensuring effective implementation of information security policies and procedures

3. Scope

This policy is applicable to all departments and users of IT resources, assets and applies to users of any system's information or physical infrastructure and third-party's systems used by the BESSEGGEN as mandated by regulatory agencies CERT-IN, SEBI and ISO 27001:2013.

4. Policy Statement

BESSEGGEN shall prepare and implement security risk requirements and procedures to mitigate risk and provide direction so that BESSEGGEN network remains secure and not vulnerable to threats.

Refer: Risk Management guidelines as per [ISO/IEC 27001]

5. Terms used and Definition

SN	Terms	Definitions

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

1	**Guidelines**	To identify how physical and logical security will be provided for hardware and software assets (locks, passwords, virus protection, etc.).
2	**Risk**	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence Asset
3	**Criticality**	Criticality is the quality, state, or degree of being of the highest importance
4	**Risk Analysis**	A systematic use of information to identify sources and to estimate risk.
5	**Risk Assessment**	The overall process of risk analysis and risk evaluation, where risk analysis is defined as the systematic approach to identify an organization's exposure to uncertainty and to estimate the risk.
6	**Threat**	A potential to cause an unwanted incident which may result in harm to a system such as unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin
7	**Non-Disclosure Agreements (NDA)**	A legally binding document which protects the confidentiality of ideas, Designs, plans, concepts, or other commercial material.
8	**Security breach**	Violation of any security policy or procedures.
9	**Risk Treatment**	A process of selecting and implementing measures to change, modify or lower risk
10	**Information Security**	A process of safe-guarding information assets from unauthorized access, modification, use, disruption, and destruction to ensure confidentiality, integrity, availability, and non-repudiation of information.
11	**Information Security Event**	An event that is caused due to any action on an Information Asset. For example, deleting a key file from a critical business system.
12	**Information Security Incident**	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
13	**Intrusion**	An uninvited and unwelcome entry into a system by an unauthorized source.
14	**Key Management**	In cryptography, it is the creation, distribution, and maintenance of a secret key. It determines how secret keys are generated and made available to both parties; for example, public key systems are widely used for such an exchange. If session keys are used, key management is responsible for generating them and determining when they should ne renewed

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

6. Roles and Responsibilities:

SN	Roles	Responsibilities
1	CISO	To establish policy so that it protects people, assets, infrastructure and technology.
2	IST Ambassador	Coordinate the activities not only within organization as well with external bodies for information security standards and guidelines related updates.
3	Manager Compliance	Coordinate with regulatory and government agencies for information security standards, guidelines compliance and audit processes.
4	Manager Security Operations	Information security managers are responsible for ensuring that all security programs, tools, and technologies are working correctly, as well as providing the necessary protections to the company's networks, digital communications, and databases
5	Manager ISPP	Conduct regular audits of policies, procedures and controls to make sure they are being adhered to standards as per regulatory authorities.
6	IT Head	Lead, manage, and govern the information assets are adequately protected, safely guarded and disposed-off as per data security guidelines and regulatory requirements.
7	Head Finance	Creating forecasting models, assessing risk in investments and ensuring all accounting activities comply with regulations.
8	HR Head	For leading and ensuring assets are returned back after the exit of an employee, termination, or transfer to different business units in the organization.
9	BU Head	Lead, manage, and govern the acquisition and application of assets within the business unit of the organization.
10	BU SPOC	Works closely with teams to harvest potentially reusable assets and to integrate existing assets into their work. May also develop, evolve, support, and retire assets.

7. Risk Management Requirements:

- Chief Information Security Officer (CISO) shall define and implement risk management to ensure cost-effective protection of all BESSEGGEN systems information.
- Risk management shall assess potential business impact, evaluating threats and vulnerabilities and selecting appropriate controls to meet the business requirement for information security in a cost-effective manner
- Risk management process shall be completed in a coordinated manner and

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

involving all the stakeholders including business owners, systems owners, security analysts and other subject matter experts.
- Independent risk management shall be conducted by organizations that are separate and distinct from those responsible for operation of BESSEGGEN systems

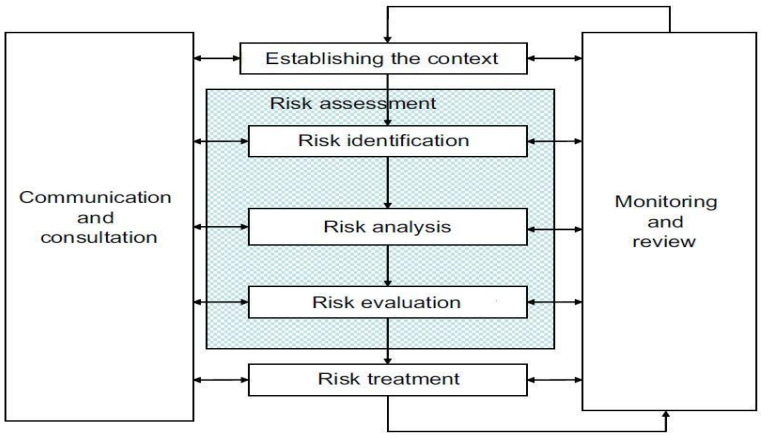
8. Risk Management Methodology

- CISO shall develop and govern risk management methodology, policies and procedures for BESSEGGEN systems protection. This risk management methodology, policies and procedures shall be based on internationally accepted standards and guidelines (e.g., ISO/IEC 27001:2013 and ISO/IEC 27005).
- BESSEGGEN shall:
    - Identify scope of risk assessment with the relevant assets.
    - Ensure that appropriate risk management measures and strategic initiatives are in place, and that they are aligned with BESSEGGEN goals.
    - Support risk management measures, strategy and associated responsibilities are clearly defined and communicated at all levels.
- The risk management methodology shall cover the following aspects:

    - Identifying and classifying assets
    - Determining asset value.
    - Identifying and assessing applicable threats to BESSEGGEN infrastructure and environment.
    - Identifying and assessing assets' vulnerability to specific threats.
    - Determining the risk
    - Identifying ways to reduce and treat those risks.
    - Prioritizing risk remediation measures

Risk Management Process (As per ISO 31000)

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)



Stage 1: Establishing the Context

This stage is the preparatory stage of the risk management process. It is focused on defining the business environment within which the entity undertaking the risk assessment operates, providing context for the assessment and the criteria against which risks will be assessed later in the process.

Stage 2: Risk Identification

This stage is focused on identifying the material risks that a department faces. It builds on the understanding of the business environment and objectives gained during stage 1 of the process and relies on inputs from top management and / or senior management and research of external and internal information sources as the principal means of identifying the risks to the Departments.

Stage 3: Risk Analysis

This stage is focused on understanding the root causes and factors that contribute to the occurrence of the identified risks and making an evaluation of the likelihood of occurrence, financial or non-financial impact of risks, and the overall risk rating. It uses a set of assessment rating scales to provide a consistent way to evaluate and rate risks across specified dimensions.

Stage 4: Risk Evaluation

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

This stage involves evaluating the residual risk (the risk remaining after considering the effectiveness of the existing controls implemented by management to mitigate the risk) to determine whether further actions are required to mitigate the risk further.

Stage 5: Risk Treatment

This stage of the process is focused on risk treatment strategies that can be applied to mitigate the identified risks.

Stage 6: Monitoring and Review

This stage of the process is focused on monitoring risks to ensure that they remain within acceptable levels.

Stage 7: Communication and Consultation

This stage of the process is focused on consolidating key information gathered throughout the risk profiling process and reporting it to the appropriate level of management and to the Board.

9. Risk Reporting Structure

Departmental Risk Coordinators

(From each Business Units) should prepare a department Risk Report on a semiannual basis based on the process outlined in this set of guidelines.

Risk Manager

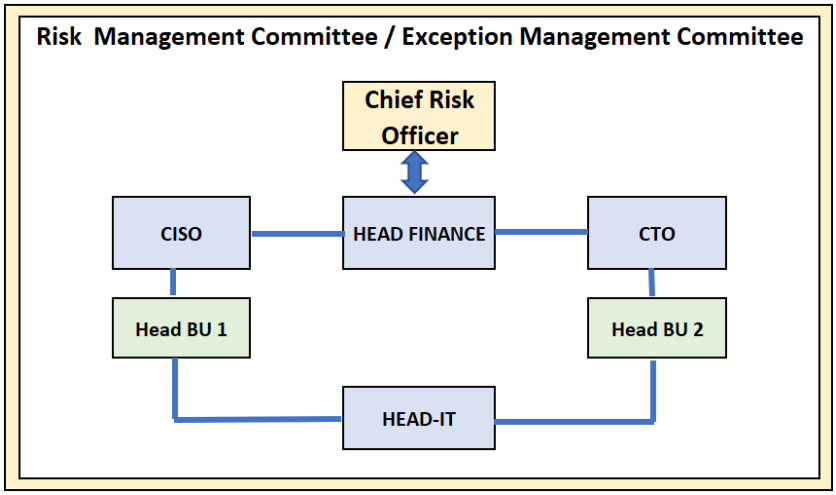
(May be part of Risk Management Committee) will work with the Department Risk Coordinators to prepare and collate the Department Risk Reports into the BESSEGGEN Final Risk Report and submit to the RMC and Board for their semiannual review, guidance, and approvals for Risk treatment / mitigation plans.

Risk Management Committee (RMC)

- Having CISO, CTO, Head Finance, Head IT, Head HR and Head Business its members and Chief Risk Officer as its Head to define:
- Risk appetite of the organization.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

- To review the risk profile of the organization to ensure that risk is not higher than the risk appetite determined by the board.
- To assist the Board in setting risk strategies, policies, frameworks, models and procedures in liaison with management and in the discharge of its duties relating to corporate accountability and associated risk in terms of management assurance and reporting.
- To review and assess the quality, integrity and effectiveness of the risk management systems and ensure that the risk policies and strategies are effectively managed.
- To review issues raised by Internal Audit that impact the risk management framework.
- To ensure that infrastructure, resources, and systems are in place for risk management is adequate to maintain a satisfactory level of risk management discipline.
- Looks in to Exception Management approvals and guidance also from Risk perspective



10. Risk Assessment

BESSEGGEN shall:

- Conduct (or have been conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

processes, stores, or transmits.

- Document risk assessment results in annual Risk Assessment.
- Review risk assessment results quarterly.
- Disseminate risk assessment results to stakeholders.
- Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

10.1 Risk Identification

- Primarily on input from top management and / or senior management and their direct reports. Their knowledge of the business is a crucial input in the risk identification process and may be obtained through meetings and/or workshops administered by the Department Risk Coordinator.
- Relevant internal information (business risk analysis, major incident reports, compliance to risk tolerances, internal audit reports, reviews by third parties, etc.).
- External information (industry or technical risk analysis, competitor reports, etc.).

10.2 Risk Analysis

The Risk analysis stage involves an assessment of the nature, likelihood, and impact of the inherent and residual risk that the business faces. Risk analysis involves, in order of occurrence:

- Consideration of the root causes and sources of risk.
- Assessment of the inherent likelihood of a risk occurring, and the potential impact if it did occur (both financial and non-financial).
- The identification of the existing controls in place to mitigate risks.
- Assessment of the effectiveness of the existing controls.
- Assessment of the residual likelihood of the risk and its potential impact.
- Determination of the overall inherent and residual risk ratings.

Inherent Risk: is defined as the level of risk faced by the business by virtue of the business it conducts and the business environment and markets in which it operates, before considering the mitigating impact of any mitigating controls implemented by management.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Residual risk: is the level of risk remaining after considering any controls already implemented, and the actual effectiveness of those controls in mitigating the risks.

Risk Root Cause Analysis: Risk "root cause" analysis helps identify the primary causes or factors contributing to the occurrence of a risk. A thorough understanding of the root causes (or risk sources) will assist in considering whether existing controls mitigate the likelihood of risks occurring or their impact should they occur, and how effective they will be.

10.3 Risk Evaluation

Risk Evaluation involves decisions on whether the current residual risk level is at the desired Target Risk level. BESSEGGEN consider:

- What is the business' risk appetite or operational loss threshold?
- Does the BESSEGGEN intend to accept the current level of risk?
- What is the cost/benefit trade-off for strengthening controls versus maintaining a reduced level of risk?
- Are there any offsetting risks or risk mitigations elsewhere in the BESSEGGEN which has already reduced the risk from the perspective of the BESSEGGEN as a whole?

11. Risk Treatment and Acceptance

- Risk Mitigation involves identifying a range of options for treating risks, assessing those options given the resources available to the Departments or function, and ultimately selecting and implementing the preferred treatment option.
- The decision on the risk mitigation option to adopt should be driven by the extent of risk that the Organization or Departments is willing to take. This should aim to reach a point as low as reasonably practicable, and references can be made to the Risk Appetite and Risk Tolerances Framework adopted by the BESSEGGEN
- Selecting the most appropriate action plans involves careful consideration and balancing of many, and sometimes competing factors. Consideration

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

should be given, for example, to the following:

- Cost and effort of implementing a planned mitigation against the derived benefits
- Legality or regulatory impact of the option
- Impact on the BESSEGGEN 's reputation
- Social responsibility factors
- Impact of a proposed response on other risks or stakeholders

- There are four high level options that can be selected to mitigate risks as outlined in the table below -

Option	Explanation of option	Illustrative actions
Accept	Accept the residual level of risk	Making a conscious decision not to take any further action.
Transfer	Involves another party bearing or sharing part of the risk	Such as through insurance, joint ventures, outsourcing contracts, supplier contracts. Risk transfer usually involves a cost or risk premium. It may also leave some residual risk (e.g., insurance excess) that can be better managed by the BESSEGGEN
Reduce	• Eliminate source of risk • Reduce the likelihood of risk occurring, • Minimize the impact of risks	• ***To reduce likelihood****:* quality assurance procedures, preventative maintenance, standard operating procedures. • **To reduce impact:** network redundancy, foreign exchange hedging, business continuity planning, crisis management, contract terms and conditions.
Avoid	Avoid an unacceptable risk.	Do not start an activity or stop a current activity.

12. Risk Management Maintenance and Review

Ongoing monitoring of risk is a critical step in the process and is to be integrated into business practices and business management routines. Regular monitoring should address whether:

- Planned actions are progressing as intended and in accordance with the planned timetable, are appropriately resourced and continue to be appropriate
- Changing circumstances have altered risk priorities and risk ratings levels
- New or emerging risks have been identified (and risk ownership assigned), and

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

- Any assumptions made in making a risk assessment continue to be valid.

Risk monitoring should be:

- Built into standard operating procedures as appropriate
- Included as a standard agenda item in periodic management meetings.

13. Communication and Consultation

Communication and consultation with external and internal stakeholders are fundamental to an effective risk management process and should take place during all stages. Those accountable for implementing the risk management process and stakeholders must understand the basis on which decisions are made, and the reasons why particular actions are required.

Risk Reporting-
Risk Reporting is the communication of the risk profile of a business or activity and the status of progress and activity occurring within the risk profile to the appropriate Business Units, RMC, and Board. This step also includes completion of the documentation of the information captured throughout the risk management process. In addition to the immediate and often more informal communication and escalation of risks and issues identified in the usual course of day-to-day work practices, formal risk reporting also occurs on a structured basis and scheduled basis at various levels within the BESSEGGEN. The report provided by each level is signed off by the relevant Management in that level and provides the basis for an aggregated risk report at the next level. Reporting of key risks is to be based on the status of the risk profile and activity with a clear focus on:

- Changes since the last reported risk profile (including the results of any independent assurance on the risks e.g., internal audit reports)
- New or emerging risks
- Factors contributing to changes in the risk profile, and the actual and planned management of the risk
- Status of (including delays to) implementation of risk treatment plans

14. Exception Management

Exceptions to the guiding principles in this policy must be documented and

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)

formally approved by the CISO/Management and exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by the CISO/Management.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3 ,FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301LLP, IDENTIFICATION NUMBER: AAM-6165 (2018-19)