JSE Clear

Enterprise Risk Management Framework

February 2023

Contents

VERSION CONTROL

Issue date	February 2021
Owner	JSE Clear Chief Risk Officer
Document type	Framework
Version	Final V5.0
Approved by	JSE Clear Risk Committee

VERSION HISTORY

Version	Date	Summary of changes	Author
1.0	November 2015	Framework creation	Post-trade Services Division
1.1	April 2016	Annual Review	Post-trade Services Division
1.2	July 2017	Annual Review	Post-trade Services Division
1.3	July 2018	Annual Review	Post-trade Services Division
1.4	July 2019	Annual Review	Post-trade Services Division
2.0	February 2020	Annual Review	Post-trade Services Division
3.0	February 2021	Annual Review	Post-trade Services Division
4.0	February 2022	Annual Review. Update of risk rating scale from 4x4 to 5x5 matrix in line with risk management best practice and alignment to JSE Group.	JSE Clear Risk
5.0	February 2023	Annual Review and minor changes.	JSE Clear Risk

1 INTRODUCTION

The purpose of this document is to articulate JSE Clear's (JSEC) risk management philosophy and the various policies that underpin this. JSEC's risk management principles, governance and the key enterprise risk management processes are described. Brief overviews of the individual supporting risk policies are provided. JSEC's risk management approach considers those risks associated directly with clearing activities in the derivatives market and with the overall JSEC business.

JSEC's risk management philosophy is overarching, providing an "umbrella" of principles which are applied consistently across all JSEC functions and clearing services. JSEC's enterprise risk management framework is aligned with the risk appetite set by the JSEC Board and provides principles that govern how the business manages itself against the risk appetite.

2 OBJECTIVES AND APPROACH

The objectives of the risk management framework are:

- To provide a comprehensive overview of JSEC's risk management approach;
- To record the different risks to which JSEC is exposed by operating a clearing service;
- To provide an auditable monitoring, control and management framework for both the policies and the risks;
- To support effective ownership and accountability of JSEC's risk tolerance and activities; and
- To ensure appropriate compliance with local regulation and alignment with international standards.

3 SCOPE

This framework applies to JSEC and its business in its entirety. All aspects of the operations of JSEC are covered by this framework, including those carried out by JSEC itself and those provided by third parties.

4 RISK MANAGEMENT PRINCIPLES

The following are the overarching risk management principles applicable to JSEC and the role it plays in the South African markets:

- To maintain the integrity of the South African exchange traded derivatives market by operating a licensed Central Counterparty.
- To protect and enhance JSEC's value to the market and its stakeholders.
- To ensure risks are managed appropriately to safeguard the business' objectives, and to be guided by the risk appetite established by the Board.
- To implement processes to identify, assess, mitigate and monitor risks to the business, and to ensure these processes are sufficiently robust to adapt to the changing market and operating environment.
- To be able to resolve a market participant default through utilization of available loss compensation resources in all extreme but plausible circumstances.
- To establish an appropriate risk culture which encourages a questioning mindset, critical assessment of practices and processes and transparent provision of information, and to empower employees to all act as risk managers.

- To apply an unambiguous system of accountability to ensure adequate and appropriate action is taken to mitigate risks, and in response to the realization of risk.
- To be compliant with local and international regulatory standards.

5 THREE LINES OF DEFENCE MODEL

JSEC has adopted a "three lines of defence" model, and places responsibility for managing operational risk on the business as the first line of defence, with support and oversight provided by specialists Risk practitioners as second line of defence, and with assurance and validation carried out by Internal Audit as the third line of defence.

i. Business Operations (JSEC Management) - ensures risk management is part of day-to-day operations; conducts business in accordance with strategy and related risk appetite and limits; and reports and escalates risk limit breaches.
ii. Oversight function (JSEC Risk, Legal and Compliance Management) - establish risk management policies and processes and implement these throughout the business; monitors risk limits and communicates exceptions to the Executive and JSE Clear Risk Management Committee; and provides risk management insight and guidance.
iii. Internal Audit - provides independent assurance on risk management practices by the business and oversight functions.

Additional oversight is provided by the JSE Clear Executive Committee, JSE Clear Risk Committee and JSE Clear Audit Committees as well as by the JSE Exco and JSE Group Risk Management Committee.

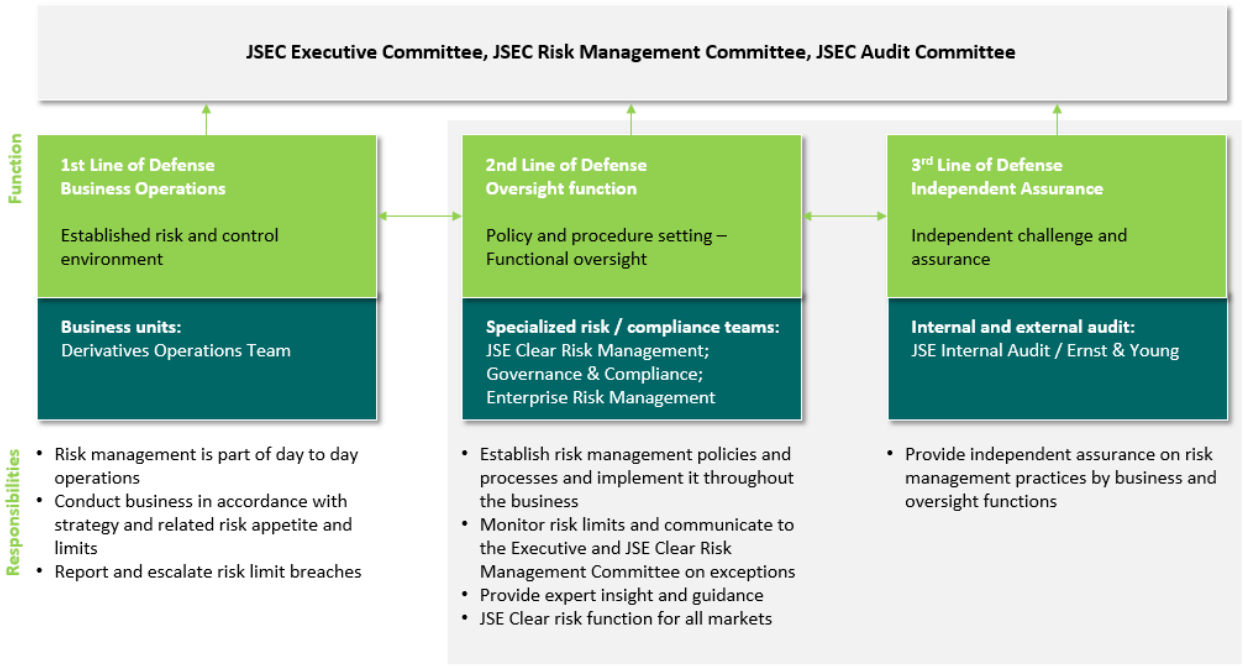


Figure 2: Roles & responsibilities matrix: the three lines of defence

JSEC Combined Assurance is achieved through the lines of defence and the oversight committees that form part of the JSEC governance structures.

6 JSE CLEAR RISKS

The key risks faced by JSE Clear are presented in the graphic below.

JSEC has defined tailored approaches for each of the components shown above, supported by a suite of policies and procedures.

Management of credit risk is tailored to reduce the probability of a key stakeholder defaulting, and minimize the losses in the event that a default does in fact occur. Mitigants applied by JSEC to manage probabilities of stakeholder defaults center on the application of strict clearing member and settlement bank requirements and credit risk monitoring, and investment risk controls. Migitants implemented to minimize losses in the case of a default include the maintenance of sufficient prefunded financial resources, and the definition of clear default management principles and processes.

JSEC's first mitigant against counterparty cleared risk is the establishment of financial and operational criteria for clearing members, supported by ongoing monitoring of adherence to these. The aim of such criteria and monitoring is to reduce the likelihood of clearing member default, thereby reducing the risk of a financial loss resulting from such a default.

JSEC maintains a robust default management policy. By putting in place effective planning, JSEC aims to minimise the losses which may arise from a clearing member default by defining upfront how such a default will be managed and by being appropriately prepared to manage such an event should it arise.

JSEC requires margining of all clearing members and maintains a 'Default Waterfall' which describes what prefunded resources are available and how these resources will be used to cover losses arising from a clearing member default. This is supported by the stress testing of exposures to ensure resource adequacy in extreme but plausible stressed environments.

JSEC establishes criteria for the risk management of settlement banks and investment counterparties to ensure that margin payments to/from JSEC are timeous, and that margin investment is robust. JSEC further safeguards against shortcomings in margin liquidity (at the time of a clearing member default) by having established its own liquidity facilities to draw upon and utilize if there is a delay in the release of margin investments. JSEC has policies addressing the management of liquidity risk and mandates for the management of investments.

JSEC's faces a range of operational risks in the execution of its business functions, including people and process failures, physical and information security, amongst others. JSEC has a suite of policies addressing the identification, management and monitoring of these operational risks, and for the recovery from operational failures through policies relating to incident management, business continuity and disaster recovery.

JSEC holds capital as a mitigant for the risks that it faces as a CCP. Capital management principles are set out in the capital management policy and capital calculation methodologies.

JSEC has a recovery and resolution policy and plan in place to address the extreme scenario that the CCP has to be resolved or wound down as a business.

Refer to Appendix A for a list of policies for the management of the abovementioned risks, mitigants and controls.

7 RISK MANAGEMENT PROCESS

The JSEC risk management process is aligned to ISO 31000 and is standardized to the extent possible throughout all functions of JSE Clear, and against all risks faced by the business.

7.1 Identification of risks

Risks are to be identified and documented. All risks are to be assigned an owner, who will typically be the employee responsible for the function in which the risk has arisen. A risk log is to be maintained and should contain a description of the risk and information relating to how the risk will be managed (as described below). The identified risks are to be reviewed at least every 6 months, or after a change in the business or operating environment. Existing risks must be assessed to determine whether they are still relevant and whether their ratings have changed, and any new risks that may have arisen must be included. The risk log must be presented to the Risk Committee every 6 months.

7.2 Assessment of risks

All identified risks are to be assessed and rated by applying a standard rating methodology (refer to Appendix B). The risk rating is to consider the likelihood of the risk occurring and the impact to the business should the risk occur. Risks may impact the business in different ways, e.g. operational impact or financial impact, and the rating of the most severe impact should be adopted.

Risks are to be assessed on both an 'inherent' and 'residual' basis. The inherent risk rating is the rating of risk likelihood and severity if no mitigants are considered. The residual risk rating takes into account the likelihood and severity of the risk after mitigants and controls have been implemented. Examples of control activities are reconciliations, review of performance, segregation of duties etc.

Risks should also be assessed in terms of their velocity – i.e. the speed of onset of the risk and how quickly JSEC will feel the impact if the risk materializes.

Risks are also assessed in terms of the urgency required to address the risk. The urgency determines how quickly JSEC should respond to this risk.

7.3 Response to risks

A response plan must be defined for each risk identified. The plan should include the actions to be taken to manage the risk, the person responsible for implemented the action, and the due date of the action. Ongoing monitoring of the response plan is required to report on the status of completion of the action and the effectiveness thereof.

Responses to risks typically can be categorized as follows:

i. Avoid - Action taken to ensure that the probability or impact of a threat is eliminated. Avoidance actions include e.g. change business plan to eliminate the risk or relax the business objective that is in jeopardy.
ii. Transfer - Action to allocate ownership for more effective management of a risk. Transferring risk involves finding another party who is willing to take responsibility for the management, and who will bear the liability of the risk should it occur. The risk is then owned and managed by the party best able to deal with it.
iii. Mitigate - Action taken to reduce the probability and/or the impact of a risk to an acceptable level. Mitigation or acceptance strategies are most often used since the number of risks that can be addressed by avoidance or transfer are usually limited. Examples of mitigation strategies include e.g. adopting less complex processes, automation, conducting more tests, developing a prototype, designing redundancy into a subsystem that may reduce the impact from a failure of the original component.
iv. Accept - Accepted risks are risks that remain after response actions and risks for which response is not cost effective or practical. The governance required for risk acceptance is determined by the severity of the risk. Acceptance of risks rated medium may be approved by the JSEC Chief Executive Officer and the JSEC CRO. Acceptance of risks rated high and extreme must be approved by the JSEC Risk Committee.

7.4 Monitoring and reporting of risks

The risk log and all the associated parameters describing the risk and plans to manage the risk must be monitored on an ongoing basis and must be formally updated at least 6 monthly. The nature of the risk will determine the frequency of monitoring, with some risks requiring daily monitoring and others monthly monitoring. The risk owner is responsible for monitoring and reporting on the status of the risk.

JSEC's risk profile including assessment of the risk appetite status (measurements against thresholds) and assessment of JSE's strategic risks shall be reported quarterly to the JSEC Risk Committee, and the risk log shall be presented 6 monthly.

8 ROLES AND RESPONSIBILITIES

The stakeholders as set out in the table below have more specific roles and responsibilities with regards to the development, oversight, assurance and management of risks.

ROLES	RESPONSIBILITIES
JSEC Board	The JSEC Board is ultimately responsible for the governance of operational risk and determining the adequacy and effectiveness of the risk management process. The Board delegates the governance and oversight of JSEC risks to the JSEC Risk Committee. The Board delegates the responsibility for day-to-day management of the operations and overall enterprise risk of JSEC to the Chief Executive Officer (CEO).
JSEC Risk Committee	The JSEC Risk Committee, evaluates, monitors and directs risk and opportunity management at JSEC by ensuring that risk and opportunity management forms an integral part of day-to-day operations. The committee executes its function through review, evaluation, monitoring and approval of: • Changes in risk policies and methodologies; • Risk management action plans; • Risk profiles supported by key indicators; • Strategic risks; • JSEC incidents/loss events; • Compliance deviations creating risks; and • Assurance findings resulting in significant risks. The Chairperson of the JSEC Risk Committee reports to the Group Risk Management Committee (GRMC) on all categories of risk applicable to JSEC on a quarterly basis.
JSEC Chief Executive Officer (CEO)	The CEO ensures that the operations of JSEC are managed within the appetite set by the Board and is primarily responsible for establishing the control environment within which JSEC operates. The CEO ensures that there are adequate controls in place for the risks to which JSEC is exposed.
JSEC Chief Risk Officer (CRO)	The CRO, supported by the Risk team has the following responsibilities: • Develop, maintain and promote appropriate risk policies, framework, approach and culture, as well as methodologies, processes and support systems; • Provide oversight and reporting of the risks faced by JSE Clear; and

ROLES	RESPONSIBILITIES
	• Support business functions in meeting the requirements of the risk policies, and in adopting a suitable risk culture amongst employees.
JSEC Chief Operations and Information Officer (COO/CIO)	The COO/CIO ensures that the operations of JSEC are managed within the appetite set by the Board by: • Identifying and owning risks that manifest in the operational processes and infrastructures of JSE Clear; and • Ensuring that third party service providers adhere to the minimum risk management standards required by JSEC and monitor their performance.
JSEC Chief Compliance Officer (CCO)	The JSEC CCO oversees and manages compliance risks and opportunities within JSEC by ensuring: • JSEC is in compliance with various applicable regulatory and compliance standards; and • JSEC staff members adhere to regulatory requirements, internal procedures and policies.
Internal Audit	• Perform risk-based audits using the risk registers to inform the internal audit plan; • Assess the adequacy and effectiveness of the risk management process, and of controls.

9 GOVERNANCE

The JSEC Board has delegated responsibility for the oversight of JSEC risk management to the JSEC Risk Committee. Various policies, processes and reports are in place to provide JSEC Risk Committee with sufficient information to determine whether the JSEC risks are being effectively managed and mitigated.

The JSEC Risk Committee will recommend the initial approval of this Framework by the JSEC Board or when there are material changes. The regular annual review of this Framework, and its underlying policies, will be approved by the JSE Clear Risk Committee.

10 APPENDIX A: LIST OF RISK POLICIES

1. JSE Clear Default Fund Policy
2. JSE Clear Default Management Policy
3. JSE Clear Business Continuity Management Policy
4. Recovery and Resolution Policy
5. JSE Clear Operational Risk Policy
6. JSE Clear Initial Margin Policy
7. JSE Clear Intraday Margin Call Policy
8. JSE Clear Stress Testing Policy
9. JSE Clear Counterparty Credit Risk Monitoring Policy
10. JSE Clear Liquidity Policy
11. JSE Clear Collateral Policy
12. JSE Clear Capital Management Policy
13. JSE Clear Investment Mandate (IM and Default Fund)
14. JSE Clear Investment Mandate (Own Funds)

11 APPENDIX B: RISK RATING METHODOLOGY

Enterprise and operational risks are to be evaluated according to the probability of occurrence and the potential impact given their occurrence. Impact could take a number of forms including a financial loss, a decrease in income, reputational damage or a regulatory sanction.

Rating Scales

Likelihood:

Rating	Assessment	Description
1	Rare	Only to occur in extreme circumstance. More likely not to occur under normal circumstances; < 15% chance of occurring.
2	Unlikely	Occurs infrequently and unlikely to occur within 3 years. Given time, the risk is unlikely to occur; 15 – 25% chance occurring.
3	Possible	Above average chance that the risk will occur at least once in the next 3 years. There is a possibility of the risk occurring; 25 - 50% chance of occurring.
4	Likely	Could easily occur and is likely to occur at least once within the next 12 months. It is likely for the risk to occur under most circumstances; 50 - 75% change of occurring.
5	Probable	The risk is already occurring, or likely to occur more than once within the next 12 months. > 75% chance of occurring.

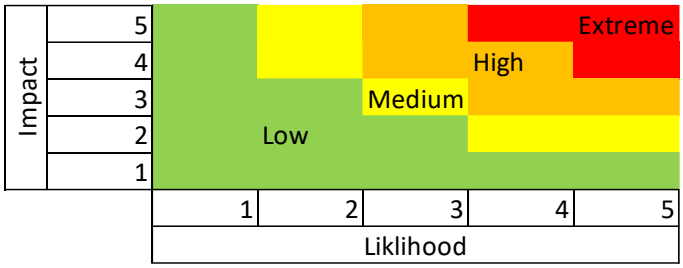
Impact:

Rating	Assessment	Description
1	Insignificant	A risk event that, if it occurs, will have little or no impact on the achievement of the objectives.
2	Minor	A risk event that, should it occur, will have a minor impact on the achievement of objectives but will still be within the acceptable tolerance levels.
3	Moderate	A risk event that, should it occur, will have a moderate impact on the achievement of objectives. The achievement of one or more objectives might be impacted. The impact is still within the minimum acceptable tolerance levels.
4	Major	A risk event that, should it occur, will have a major impact on the achievement of objectives. The achievement of more than one objective might be impacted. The impact of the event will lead to a breach in the acceptable tolerance levels.
5	Extreme	A risk event that, should it occur, will have an extreme impact on the achievement of objectives. The impact of the event will lead to a significant breach in the acceptable tolerance levels.

Risk Matrix

In order to calculate an overall risk rating the following 5x5 rating is used:

Impact Scale		Liklihood scale	
#	Description	#	Description
1	Insignificant	1	Rare
2	Minor	2	Unlikely
3	Moderate	3	Possible
4	Major	4	Likely
5	Extreme	5	Probable



Resultant Risk Rating

Rating	Description
Low	**Risk**: On the JSEC 5x5 risk rating scale these are risks of a value of 1-6. Risks with a residual rating within this range are not a concern for the JSEC. **Indicator**: Values falls within acceptable range. **Assurance/Audit**: Well controlled with no findings or findings being limited to improvements for better alignment to best practice or further maturity in operations. **Project Assurance/Oversight**: No project concerns that have enterprise level significance. **Actions for this category at an enterprise level**: Improvements are to be evaluated, but are discretionary and will not be tracked at an enterprise level. Managed and monitored routinely. Report to Risk Manager for monitoring and evaluation of controls.
Medium	**Risk**: On the JSEC 5x5 risk rating scale these are risks of a value of 7-11. Risks with a residual rating within this range require attention but do not constitute areas of concern at an organisational level. **Indicator**: Value not optimal but not an enterprise level concern. **Assurance/Audit**: Not all controls are not effective resulting in some exposure to the JSEC. **Project Assurance/Oversight**: Some project concerns but managed not making it likely to have enterprise level significance. **Actions for this category at an enterprise level**: Improvements are recommended but will not be tracked at an enterprise level. Active management, Report to CRO for monitoring and evaluation of controls.
High	**Risk**: On the JSEC 5x5 risk rating scale these are risks of a value of 12-18. Risks with a residual rating within this range are causing concern at an organisational level and require action. **Indicator**: Value causing concern at an organisational level and indicates a risk or control area that needs to be addressed. **Assurance/Audit**: Limited assurance can be given with significant control area weaknesses resulting in notable enterprise risk. **Project Assurance/Oversight**: Enterprise level significant project issues and impact. **Actions for this category at an enterprise level**: Improvements are to be actioned and will be tracked at an enterprise level. Pro-active management. Risk To be escalated to Executive. Action plan development required.
Extreme	**Risk**: On the JSEC 5x5 risk rating scale these are risks of a value of 19-25. Risks with a residual rating within this range must be addressed as a priority due to high JSE exposure. **Indicator**: Value indicating high JSE exposure that needs to be addressed as a priority. **Assurance/Audit**: Insufficient assurance can be given with critical control area weaknesses resulting in unacceptable enterprise risk. **Project Assurance/Oversight**: Enterprise level significance project issues with major enterprise impact.

Rating	Description
	Actions for this category at an enterprise level: Improvements must be prioritised at an enterprise level. Urgent and immediate action required. Risk to be escalated to board for attention. Action plan development required.

Risk Velocity – Speed of Onset

Risk velocity is how fast a risk materialises and impacts the JSE. It is the length of time it takes for a risk to move from the initial cause through to experiencing the impact. It is a time-based dimension.

Velocity Rating	Description
Immediate	Immediate impact (within 7 days)
Quarter	Within next quarter
Year	Within 3 - 12 months
Medium term	Medium term impact (> 12 months)

Urgency Response Rating

Urgency indicates the time frame within which the JSE must act to address the risk. Risk treatments include reduction, avoidance, transfer, acceptance or sharing. In the case of risks out of the control of the JSE, the lowest rating is used (MT). It is a time-based dimension.

Urgency Response Rating	Description
Immediate	Immediate action required to address risk
Quarter	Action required within the next quarter action required
Year	Action required within the next year
Medium term	Medium-term action required OR no controls are possible

Control Adequacy and Effectiveness

The following scale is used in rating control adequacy and effectiveness in both risk ratings as well as assurance/audit evaluations.

Control Adequacy	Description
Adequate	The control(s) is designed to address the risk.
Inadequate	The control(s) is not in place or not designed to address the risk.

Control Effectiveness

The following scale is used in rating control effectiveness in both risk ratings as well as assurance/audit evaluations.

Control Effectiveness	Description
Effective	The control(s) applied is designed and functioning appropriately.
Partially Effective	The control(s) applied is functioning with some discrepancies.
Ineffective	The control(s) applied is not contributing to the management of the risk.

Control Effectiveness	Description
Inadequate	The control(s) is not in place or not designed to address the risk.

12 APPENDIX C – GOVERNANCE COMMITTEE ACTIONS

No.	Ref	Action Item	Frequency	Applicable Governance Forum
1.	7.3	Response to Risks Acceptance of risks rated high and extreme must be approved by the JSEC Risk Committee.	As required	• JSE Clear Risk Committee
2.	8	Roles and Responsibilities The Chairperson of the JSEC Risk Committee reports to the Group Risk Management Committee (GRMC) on all categories of risk applicable to JSEC on a quarterly basis.	Quarterly	• JSE Clear Risk Committee Chairman
3.	9	Governance The JSEC Risk Committee will recommend the initial approval of this Framework by the JSEC Board or when there are material changes. The regular annual review of this Framework, and its underlying policies, will be approved by the JSE Clear Risk Committee.	Annual	• JSE Clear Risk Committee • JSE Clear Board