ISO 31000:2018 Risk Assessment Pack

Part of the ISRR Toolkit

IRMSA TECHNICAL LIBRARY

Disclaimer

The Institute of Risk Management South Africa (IRMSA) has prepared this material for general information and educational purposes only. It does not constitute professional advice, consultancy, assurance, legal opinion, financial advice or any other form of professional service, and should not be relied upon as such. Users of this material should obtain appropriate professional or specialist advice before taking, or refraining from taking, any action based on its content.

While reasonable efforts have been made to ensure that the information contained herein is accurate and up to date at the time of publication, IRMSA gives no representations, warranties or guarantees, whether express or implied, as to the completeness, accuracy, reliability, suitability or availability of the information, guidance, tools or examples provided. Any reliance placed on this material is strictly at the user's own risk.

To the fullest extent permitted by applicable law, IRMSA, its officers, employees, members, contributors and agents shall not be liable for any loss, damage, liability, costs or expenses of any nature whatsoever, whether direct, indirect, special, consequential or otherwise, arising out of or in connection with the use of, or reliance on, this material or any decision made, action taken or omission based on it.

Reference in this material to any specific organisations, frameworks, standards, products or services does not constitute endorsement or recommendation by IRMSA, nor does it imply that they are the only or the most appropriate sources available. IRMSA reserves the right to amend, update or withdraw this material at any time without prior notice.

Use of this material is subject to the laws of the Republic of South Africa and any applicable international instruments. Users remain solely responsible for ensuring that their own policies, frameworks and practices comply with all relevant legal, regulatory and governance requirements in the jurisdictions in which they operate.

Contents

Executive Overview

This Risk Assessment Pack provides structured templates and guidance for implementing ISO 31000:2018 Risk Management across an organisation. The pack covers the complete risk management lifecycle: scope and context definition, risk identification, analysis, evaluation, and treatment planning.

Document Purpose: To enable effective, consistent risk assessment aligned with international best practice (ISO 31000:2018) and integrated with strategic and resilience objectives.

Applicable Standard: ISO 31000:2018 – Risk Management – Principles and Guidelines

Alignment: IRMSA Guideline on Integrating Strategy, Risk and Resilience (2022); Institute of Directors King V Code of Governance

Part 1: Risk Management Fundamentals

1.1 ISO 31000:2018 Framework Overview

ISO 31000:2018 establishes principles, framework, and process for risk management across all sectors and organisations. The standard comprises three core elements:

Element	Description
Principles	11 underpinning principles guiding risk management (e.g. integrated, structured, dynamic, inclusive)
Framework	Governance, roles, relationships, processes within organisation context
Process	Scope/context → Identification → Analysis → Evaluation → Treatment → Monitoring

Table 1: ISO31000 Standard Components

1.2 Key Principles (ISO 31000:2018)

1. **Integrated** – Risk management integral to all organisational activities
2. **Structured and comprehensive** – Systematic approach with clear methodology
3. **Customised** – Tailored to organisational context and objectives
4. **Inclusive** – Informed by and considering stakeholder perspectives
5. **Dynamic** – Responsive to changing internal and external conditions
6. **Evidence-based** – Using best available information and expertise
7. **Transparent** – Clear communication and reporting of risks
8. **Human and cultural** – Recognising human factors and organisational culture
9. **Continuous improvement** – Iterative refinement of risk management
10. **Relationship-focused** – Considering stakeholder interdependencies
11. **Value creation and protection** – Balancing opportunity and threat management

1.3 Risk Management Roles & Responsibilities

Role	Accountability	Key Responsibilities
Board / Governing Body	Overall risk governance; risk appetite approval	Set risk culture; approve framework; oversee reporting
Chief Executive Officer	Risk management mandate; organisational integration	Embed risk culture; align strategy with risk appetite
Chief Risk Officer / Head of ERM	Risk process ownership; framework management	Facilitate assessments; maintain risk register; report to Board
Business Unit Heads	Operational risk ownership; context definition	Identify risks within remit; implement treatments; report status
Risk Champions/Coordinators	Cross-functional risk support; data collection	Support identification process; maintain documentation
Internal Audit	Independent assurance; process review	Assess framework effectiveness; audit treatments
External Audit / Regulators	External assurance; compliance verification	Verify compliance with standards and regulations
All Employees	Risk awareness; incident reporting	Identify emerging risks; report near-misses and incidents

Table 2: Risk Management Roles and Responsibilities

Part 2: Scope & Context Definition (Step 1 of Risk Process)

2.1 Risk Assessment Scope Definition

Before identifying and assessing risks, clearly define the boundary and context of the risk assessment.

Scope Parameter	Detail
Assessing Scope	[e.g. Division, Business Unit, Function, Project, Process]
Geographic Scope	[e.g. South Africa, Sub-Saharan Africa, Global]
Time Horizon	[e.g. 1 year, 3 years, 5 years]
Stakeholders Included	[e.g. Executives, Business Unit Heads, Process Owners, Employees]
Assessment Method	[e.g. Workshop, Interviews, Surveys, Data Analysis]
Facilitation Team	[e.g. CRO, Risk Team, Internal Audit]
Assessment Date(s)	[Date(s) of workshop(s) or interviews]
Last Review/Update	[Date of last assessment]
Next Scheduled Review	[Date for next assessment cycle]

Table 3: Risk Assessment Scope Definition

2.2 Organisational Context Assessment

Understanding the organisation's external and internal context is critical to identifying relevant risks and establishing risk criteria.

External Context

External Context Factor	Current State	Risk Implication
Regulatory Environment	[Regulatory requirements, compliance obligations]	[Compliance, operational risk]
Competitive Landscape	[Market structure, competitor positioning]	[Market/strategic risk]

External Context Factor	Current State	Risk Implication
Economic Conditions	[Macro trends, interest rates, inflation]	[Financial, strategic risk]
Technology Trends	[Digital disruption, cybersecurity]	[Operational, strategic risk]
Social/Stakeholder Expectations	[Community, employee, customer expectations]	[Reputational, operational risk]
Environmental/Climate Factors	[Climate change, resource scarcity]	[Operational, supply chain risk]
Geopolitical Volatility	[Trade, sanctions, political instability]	[Strategic, market access risk]

Table 4: External Context Assessment

Internal Context

Internal Context Factor	Current State	Risk Implication
Organisational Structure	[Centralised/ decentralised; hierarchies]	[Governance, operational risk]
Strategy	[Strategic direction; key objectives; KPIs]	[Strategic alignment; goal achievement]
Culture	[Risk-aware culture; tolerance for incident reporting]	[Behavioural risk; reporting quality]
Governance	[Board oversight; committee structure; policies]	[Governance risk; control effectiveness]
Financial Position	[Revenue, profitability, leverage, liquidity]	[Financial resilience; investment capacity]

Internal Context Factor	Current State	Risk Implication
Technology/Systems	[IT maturity; cyber resilience; data management]	[Cyber, operational, strategic risk]
Talent/Capability	[Skills, leadership pipeline, retention]	[Operational, strategic risk]

Table 5: Internal Context Assessment

2.3 Risk Criteria Establishment

Risk criteria define how risks will be evaluated and prioritised. Criteria should align with organisational strategy and stakeholder expectations.

Risk Criteria	Definition
Risk Categories	[e.g. Strategic, Financial, Operational, Compliance, Reputational, Cyber]
Likelihood Scale	[e.g. 1=Rare (1-10 yrs), 2=Unlikely (10-25 yrs), 3=Possible (5-10 yrs), 4=Likely (1-5 yrs), 5=Very Likely (<1 yr)]
Impact Scale	$ | Operational | Reputational | Compliance | Strategic [e.g. 1=Negligible ($0-1M loss), 2=Minor ($1-5M), 3=Moderate ($5-20M), 4=Major ($20-50M), 5=Catastrophic (>$50M)]
Risk Tolerance Bands	[Acceptable, Manageable, Unacceptable by category and impact level]
Scoring Methodology	[Likelihood × Impact; weighted scoring; heat map placement]
Interdependencies	Consider correlated/cascading risks [e.g. Cybersecurity breach → Reputational + Financial]

Table 6: Risk Criteria Definition

Part 3: Risk Identification (Step 2 of Risk Process)

3.1 Risk Identification Process

Risk identification uses multiple techniques to surface known, emerging and uncertain risks across the organisation.

3.1.1 Risk Identification Techniques

Technique	Application	Output
Brainstorming Workshops	Cross-functional group identifies risks using prompts and structured discussion	Risk list with brief descriptions
Interviews	One-on-one conversations with key executives, process owners, subject matter experts	Risk narratives, context, owner perspective
Checklists/Questionnaires	Standardised risk categories (compliance, cyber, supply chain, etc.) with targeted questions	Structured risk catalogue
Historical Data Analysis	Review of past incidents, near-misses, audit findings, claims	Evidence-based risk patterns
Scenario Planning	Development of plausible future states (best case, base case, downturn) to surface potential risks	Forward-looking risk narratives
SWOT/PESTEL Analysis	Systematic review of Strengths, Weaknesses, Opportunities, Threats; Political, Economic, Social, Tech, Environmental, Legal	Strategic and external risks
Process Mapping/Flow Analysis	Visual documentation of process steps, hand-offs, dependencies to identify failure points	Operational risks, control gaps

Technique	Application	Output
Expert Workshops	Engagement of external experts (consultants, industry peers, academics) for emerging risk insights	Emerging/horizon risks
Benchmarking	Comparison of risks faced by peer organisations in similar sectors/markets	Industry-specific risk awareness
Incident/Audit Log Review	Analysis of historical incidents, audit findings, regulatory feedback	Validated risk patterns

Table 7: Risk Identification Techniques

3.2 Risk Identification Register Template

Use this template to capture all identified risks during the identification phase.

Risk ID	Risk Category	Risk Title	Risk Description	Potential Cause(s)	Source/ Trigger
[R-001]	[Strategic/ Financial/ Operational]	[Concise risk title]	[What could go wrong? Impact?]	[Root cause(s)]	[How/ where identified]
[R-002]	[ ]	[ ]	[ ]	[ ]	[ ]
[R-003]	[ ]	[ ]	[ ]	[ ]	[ ]

Table 8: Risk Identification Register (Phase 1 Capture)

Part 4: Risk Analysis (Step 3 of Risk Process)

4.1 Risk Analysis Approach

Risk analysis examines the nature and magnitude of risks, considering likelihood (frequency/probability) and consequences (impact), and any existing controls.

4.2 Qualitative Risk Analysis

Most organisations begin with qualitative analysis using structured scales and expert judgment.

4.2.1 Likelihood Assessment Scale

Likelihood Level	Descriptor	Frequency/Probability	Example
1	Rare	<10% probability; <1 in 10 years	Once or never in organisational history
2	Unlikely	10-25%; 1 in 10-25 years	Known to occur in industry but not this organisation
3	Possible	25-50%; 1 in 5-10 years	Has occurred in organisation or is foreseeable
4	Likely	50-75%; 1 in 1-5 years	Multiple occurrences in organisation or regularly in industry
5	Very Likely	>75%; <1 year or annually expected	Expected to occur multiple times per year or ongoing

Table 9: Likelihood Assessment Scale

4.2.2 Impact Assessment Scale (Financial & Operational)

Impact Level	Descriptor	Financial Impact	Operational Impact	Other Impacts
1	Negligible	<R1M loss or <0.5% revenue	Minimal disruption; <1 day downtime	No reputational or compliance impact
2	Minor	R1-5M loss; 0.5-2% revenue	Localised disruption; 1-3 days downtime	Limited stakeholder impact
3	Moderate	R5-20M loss; 2-5% revenue	Significant disruption; 1-2 weeks downtime	Moderate reputational; regulatory attention
4	Major	R20-50M loss; 5-15% revenue	Severe disruption; 1-3 months downtime	Significant reputational damage; regulatory action
5	Catastrophic	>R50M loss; >15% revenue	Extended downtime; core business interrupted	Major reputation loss; regulatory sanction; viability risk

Table 10: Impact Assessment Scale

4.2.3 Risk Score Calculation

Risk Score = Likelihood × Impact

Example: A risk with Likelihood 3 (Possible) and Impact 4 (Major) = Score of 12/25

	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Likelihood 1	1	2	3	4	5
Likelihood 2	2	4	6	8	10
Likelihood 3	3	6	9	12	15

	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Likelihood 4	4	8	12	16	20
Likelihood 5	5	10	15	20	25

Table 11: Risk Score Matrix (Likelihood × Impact)

4.3 Inherent vs Residual Risk Analysis

Inherent Risk: Risk exposure before considering existing controls or mitigation actions.

Residual Risk: Risk exposure after implementing existing controls or treatment actions.

Risk ID	Risk Title	Inherent Score	Existing Controls/Mitigations	Residual Score
[R-001]	[Risk title]	[Likelihood × Impact]	[List controls in place]	[Likelihood × Impact post-control]
[R-002]	[ ]	[ ]	[ ]	[ ]
[R-003]	[ ]	[ ]	[ ]	[ ]

Table 12: Inherent vs Residual Risk Analysis

4.4 Control Assessment (Existing Controls Effectiveness)

For each risk, assess the effectiveness of existing controls or mitigations.

Risk ID	Existing Control/ Mitigation	Control Type	Design Effectiveness	Operating Effectiveness
[R-001]	[e.g. Policy X, System Y, Process Z]	[Preventive/Detective/Responsive]	[Strong/Adequate/Weak]	[Strong/Adequate/Weak]
[R-002]	[ ]	[ ]	[ ]	[ ]

Risk ID	Existing Control/ Mitigation	Control Type	Design Effectiveness	Operating Effectiveness
[R-003]	[ ]	[ ]	[ ]	[ ]

Table 13: Control Effectiveness Assessment

4.5 Risk Interdependencies & Cascading Effects

Identify risks that are correlated or may cascade, amplifying overall exposure.

Primary Risk	Secondary/Cascading Risk	Correlation/Dependency
[Cybersecurity breach]	[Operational disruption, Reputational damage, Regulatory action]	[High correlation – single event triggers multiple impacts]
[Supply chain disruption]	[Production delays, Revenue loss, Customer dissatisfaction]	[Sequential cascade – primary triggers secondaries]
[Market downturn]	[Liquidity pressure, Talent loss, Compliance failures]	[Correlated – macro condition amplifies operational risks]

Table 14: Risk Interdependencies and Cascading Effects

4.6 Quantitative Risk Analysis (Optional - Advanced)

For material risks, quantitative analysis using probability distributions and Monte Carlo simulation can provide more precise risk estimates.

Risk	Distribution Type	Expected Value / VaR
[Supply chain loss event]	[Beta or Triangular distribution]	[Mean R10M; 95th percentile R25M]
[Revenue volatility]	[Normal distribution]	[Mean R200M; Std Dev R15M; 95% CI R170M-R230M]

Risk	Distribution Type	Expected Value / VaR
[Project overrun]	[Triangular or Lognormal]	[Mean 120% of budget; VaR (95%) 150%]

Table 15: Quantitative Risk Analysis (Example)

Part 5: Risk Evaluation (Step 4 of Risk Process)

5.1 Risk Evaluation Approach

Risk evaluation compares risk scores against risk criteria to determine which risks require treatment and what priority they should receive.

5.2 Risk Tolerance Framework

Risk Band	Score Range	Treatment Decision	Governance
Acceptable (Green)	1-6	Monitor; routine management	Operational (Business Unit)
Manageable (Yellow)	7-12	Treat; develop action plan	Functional leadership (CFO/CRO)
Unacceptable (Red)	13-25	Urgent treatment; escalate	Executive/Board level

Table 16: Risk Tolerance Framework and Treatment Decision

5.3 Risk Evaluation Summary

Consolidate analysis results in a summary table for governance review and prioritisation.

Risk ID	Risk Title	Likeli-hood	Impact	Residual Score	Evaluation
[R-001]	[Risk title]	[1-5]	[1-5]	[Score]	[Acceptable/Manageable/Unacceptable]
[R-002]	[ ]	[ ]	[ ]	[ ]	[ ]
[R-003]	[ ]	[ ]	[ ]	[ ]	[ ]

Table 17: Risk Evaluation Summary

5.4 Risk Heat Map (Visualisation)

A heat map visually represents risk positioning against likelihood and impact criteria.

Interpretation:

- **Green (Acceptable):** Risks in bottom-left quadrant; monitor but no urgent action required
- **Yellow (Manageable):** Risks in middle band; require mitigation/treatment planning
- **Red (Unacceptable):** Risks in top-right quadrant; urgent escalation and treatment

Impact/Likelihood	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Very Likely (5)
Catastrophic (5)	[5]	[10]	[15]	[20]	[25]
Major (4)	[4]	[8]	[12]	[16]	[20]
Moderate (3)	[3]	[6]	[9]	[12]	[15]
Minor (2)	[2]	[4]	[6]	[8]	[10]
Negligible (1)	[1]	[2]	[3]	[4]	[5]

Table 18: Risk Heat Map Matrix (Green=Acceptable, Yellow=Manageable, Red=Unacceptable)

Part 6: Risk Treatment (Step 5 of Risk Process)

6.1 Risk Treatment Strategies (4 T's Framework)

For risks evaluated as "Manageable" or "Unacceptable," select one or more treatment strategies:

Treatment Strategy	Definition	Example Actions	When to Use
TREAT	Implement controls/actions to reduce likelihood or impact	Enhance policies, add process steps, invest in systems	Most risks; particularly operational and strategic
TRANSFER	Move/share risk with external party via insurance, contract, outsourcing	Insurance policies, vendor SLAs, shared liability clauses	Financial, property, liability, specialised operational risks
TOLERATE	Accept risk consciously; manage within tolerance; monitor closely	Accept downtime limits, supplier concentration within tolerance	Risks where cost to treat exceeds benefit; acceptable residual risk
TERMINATE	Eliminate risk by stopping activity or exiting business line	Exit market, divest business unit, cease product line	Risks exceeding risk appetite; unviable business models

Table 19: Risk Treatment Strategies (4 T Framework)

6.2 Risk Treatment Plan Template

For each risk requiring treatment, develop a detailed action plan.

Field	Detail
Risk ID	[e.g. R-001]
Risk Title	[Concise title]
Current Residual Score	[Likelihood × Impact]

Field	Detail
Target Residual Score	[Goal score post-treatment]
Treatment Strategy Selected	[Treat/Transfer/Tolerate/Terminate]
Treatment Action(s)	[Specific actions: e.g. "Implement data encryption protocol"; "Increase supplier redundancy to 2 qualified suppliers"]
Implementation Timeline	[Start date, milestones, completion date]
Owner/Accountable Party	[Executive or functional lead responsible]
Resource Requirements	[Budget, FTE, systems, external support]
Success Criteria / KPIs	[How will you measure effectiveness? e.g. "Zero breaches", "SLA uptime >99.9%"]
Residual Risk Post-Treatment | [Estimated L/I score after action(s) implemented]	

Table 20: Risk Treatment Plan Details

6.3 Master Risk Treatment Register

Consolidate all treatment plans in a master register for tracking and reporting.

Risk ID	Risk Title	Strategy	Treatment Action(s)	Owner	Target Date	Status
[R-001]	[Title]	[Treat/Transfer/Tolerate / Terminate]	[Action description]	[Owner name]	[DD/MM/YYYY]	[On Track/At Risk/Delayed]
[R-002]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[R-003]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Table 21: Master Risk Treatment Register

Part 7: Risk Monitoring & Reporting (Continuous)

7.1 Monitoring Approach

Risk monitoring involves ongoing tracking of risk status, control effectiveness, and early warning indicators.

7.2 Key Risk Indicators (KRIs)

KRIs are leading indicators that signal emerging risks before they materialise. They complement lagging incident/loss data.

Risk	Key Risk Indicator(s)	Threshold / Tolerance	Monitoring Frequency
[Cybersecurity]	[Failed login attempts, phishing email click rate, unpatched systems %]	[<100/month, <5%, <1%]	[Weekly]
[Supply chain]	[Supplier financial health score, delivery performance, concentration %]	[Score >70, on-time >95%, <30%]	[Monthly]
[Talent]	[Voluntary turnover rate, critical skill vacancy %, leadership pipeline]	[<10%, <5%, >2 successors]	[Quarterly]
[Liquidity]	[Cash balance, debt:equity ratio, credit facility utilisation]	[>R50M, <2.5x, <75%]	[Weekly]
[Operational]	[System uptime %, SLA compliance, incident frequency]	[>99.5%, >98%, <5/month]	[Daily/Weekly]

Table 22: Key Risk Indicators (Leading Indicators)

7.3 Risk Monitoring Report Template

Monthly/Quarterly Risk Status Report

Report Element	Content
Report Period	[Month/Quarter and year]
Executive Summary	Key changes in risk profile; escalations; treatment progress overview
Risk Heat Map Update	[Visual: Current risk positioning vs. prior period]
Key Metrics Dashboard	[KRI status; incident data; treatment completion %]
Risk Movements	Risks escalated to higher band; new risks identified; risks closed/resolved
Treatment Progress	Completion status of planned treatment actions; blockers/risks to implementation
Incidents/ Near-misses	Summary of actual loss events; root cause analysis; lessons learned
Emerging Risks	Horizon scanning; early warning signals; recommend escalation?
Regulatory/ Compliance Updates	Changes in regulatory requirements; implications for risk framework
Recommendations	Actions for Executive/Board consideration

Table 23: Risk Monitoring Report Contents

Part 8: Risk Register (Master Control Document)

8.1 Master Risk Register – Key Fields

The Master Risk Register consolidates all identified, analysed and evaluated risks with ownership and status.

Field	Purpose	Notes
Risk ID	Unique identifier for each risk	Sequential (R-001, R-002, etc.)
Risk Category	Strategic/Financial/Operational/Compliance/Reputational/Cyber	Enables filtering and reporting
Risk Title	Concise, descriptive title	Should be searchable; avoid jargon
Risk Description	What could go wrong? What are the potential consequences?	Narrative; 2-3 sentences
Root Cause(s)	Why might this risk occur?	Underlying drivers; not just symptoms
Likelihood (Inherent)	Probability/frequency (1-5 scale)	Before considering controls
Impact (Inherent)	Potential magnitude of consequence (1-5 scale)	Financial, operational, reputational

Field	Purpose	Notes
Inherent Risk Score	Likelihood × Impact	Unconstrained risk exposure
Existing Control(s)	Current mitigations/controls in place	Design and operating effectiveness
Likelihood (Residual)	Probability post-control	After existing controls
Impact (Residual)	Impact post-control	After existing controls
Residual Risk Score	Post-control exposure	Evaluated against tolerance
Evaluation	Acceptable/Manageable/Unacceptable	Based on tolerance bands
Risk Owner	Executive responsible for managing risk	Accountable for treatment
Treatment Strategy	Treat/Transfer/Tolerate/Terminate	Selected approach
Treatment Action(s)	Specific actions to further reduce risk	SMART objectives
Target Residual Score	Goal risk level post-treatment	Where will risk move to?

Field	Purpose	Notes
Implementation Timeline	Start, milestones, target completion	Realistic; linked to capacity
Treatment Owner	Who executes the treatment action	May differ from risk owner
Status	Not Started/In Progress/Complete/On Track/At Risk	Current position
Escalation Flag	Is risk escalated to Board/Audit Committee?	Based on score/ importance
Last Updated	Date of last review	Audit trail

Table 24: Master Risk Register – Field Definitions

8.2 Risk Register Example (Illustrative)

Risk ID	R-001	R-002
Category	Strategic	Operational
Title	Market disruption by digital competitors	Cybersecurity breach – customer data loss
Description	New market entrants with digital-native business models could capture market share; legacy competitors may consolidate	Unauthorised access to customer database; exposure of PII/financial data; regulatory sanction; reputational damage
Root Cause	Digital transformation pace slower than market; customer expectations shifting; competitive response	Insufficient access controls; legacy systems; skill gaps in security ops; remote work expansion

Risk ID	R-001	R-002
Likelihood (Inherent)	4 (Likely)	3 (Possible)
Impact (Inherent)	4 (Major)	5 (Catastrophic)
Inherent Score	16	15
Existing Controls	Digital roadmap exists; cloud migration underway; customer engagement programme	Firewalls, IDS/IPS, data encryption, access policies; limited SIEM; security awareness training
Likelihood (Residual)	3	2
Impact (Residual)	4	4
Residual Score	12	8
Evaluation	Manageable	Manageable
Owner	Chief Strategy Officer	Chief Information Security Officer
Treatment Strategy	Treat (accelerate digital transformation)	Treat (implement zero-trust architecture)
Treatment Actions	(1) Complete cloud migration by Q2 2026; (2) Launch AI/analytics capability by Q3 2026; (3) Expand partnership ecosystem	(1) Deploy EDR/XDR across endpoints; (2) Implement zero-trust identity; (3) Upgrade SIEM; (4) Enhance security team
Target Score	9	6
Timeline	Q1 2026 – Q4 2026	Q1 2026 – Q3 2026

Risk ID	R-001	R-002
Treatment Owner	Chief Technology Officer	Chief Information Security Officer
Status	In Progress	In Progress
Last Updated	07-Jan-2026	07-Jan-2026

Table 25: Master Risk Register – Illustrative Examples

Part 9: Integration with Strategy & Resilience (ISRR)

9.1 Risk Appetite Alignment with Strategy

Risk assessment should inform strategic decision-making and resource allocation. Conversely, strategy determines risk appetite and tolerance.

Strategic Objective	Associated Risks	Risk Appetite Implication
Grow revenue 5% annually	Market competition, technology disruption, customer acquisition cost	Moderate-High acceptance of strategic/competitive risk
Maintain margin at 15%	Cost inflation, operational efficiency, pricing power	Low-Moderate tolerance for operational and financial risk
Achieve net-zero by 2030	Supply chain transformation, capex requirements, regulatory timing	Moderate appetite for transitional/operational risk
Enhance customer satisfaction NPS to 50	Digital transformation, staff capability, process redesign	Moderate-High risk appetite for operational change
Preserve financial stability; maintain AA rating	Leverage limits, liquidity buffers, earnings volatility	Low tolerance for financial and solvency risk

Table 26: Strategic Objectives and Risk Appetite Alignment

9.2 Risk & Resilience Linkage

For risks with residual scores in the "Manageable" or "Unacceptable" band, also assess resilience implications.

Risk ID	Risk Title	Resilience Implication	Resilience Investment Required
[R-XXX]	[Operational disruption]	[Service interruption; recovery time >48 hours]	[Business continuity; disaster recovery; redundancy]

Risk ID	Risk Title	Resilience Implication	Resilience Investment Required
[R-YYY]	[Talent loss during crisis]	[Loss of critical capability; decision-making impaired]	[Succession planning; remote work capability; communication]
[R-ZZZ]	[Supply chain failure]	[Production halt; customer impact; financial loss]	[Supplier diversification; inventory; alternative sources]

Table 27: Risk-Resilience Nexus Assessment

Part 10: Governance & Reporting to Board/Audit Committee

10.1 Risk Governance Model

Governance Level	Responsibility	Reporting Cadence
Board / Audit Committee	Approve risk appetite; oversee framework; review strategy alignment	Quarterly
Executive Committee (Risk)	Monitor residual risks; approve treatments; escalate unacceptable risks	Monthly
Functional/Business Unit Leadership	Operational risk ownership; treatment execution; reporting	Weekly/Monthly
{**Risk & Compliance Function**}	Framework ownership; facilitation; reporting; independent assurance	Ongoing

Table 28: Risk Governance Structure and Cadence

10.2 Board/Audit Committee Risk Report

Quarterly Executive Summary Report to Board:

1. **Overall Risk Profile:** Current residual risk vs. risk appetite; movements since last quarter
2. **Heat Map:** Visual representation of risks by category and score
3. **Red Risks (Unacceptable):** Detail; escalations; treatment progress
4. **Treatment Progress:** On-track treatment actions; delayed items; risks to completion
5. **Emerging/Horizon Risks:** New risks identified; external drivers (regulatory, macro, etc.)
6. **KRI Dashboard:** Key metrics status; any breaches of tolerance
7. **Incidents/Lessons Learned:** Summary of loss events; root causes; corrective actions
8. **Regulatory/Compliance Updates:** Changes to risk environment; implications
9. **Recommendations:** Board-level actions or approvals required

Part 11: Special Topics in Risk Assessment

11.1 Cybersecurity Risk Assessment (Deep Dive)

Cyber Risk Category	Sub-Risks	Key Controls	Typical KRIs
Data Breach / Loss	Exfiltration, ransomware, deletion, corruption	Encryption, access controls, backup, DLP	Failed logins, phishing clicks, unpatched systems
System Availability	Outages, DDoS, malware, hardware failure	Redundancy, failover, monitoring, patching	Uptime %, RTO/RPO achievement, incident response time
Third-Party/Supply Chain	Vendor breaches, API vulnerabilities, dependency risks	Vendor assessment, contract clauses, monitoring	Vendor security posture scores, audit findings
Cloud/Infrastructure	Misconfiguration, privilege escalation, shared responsibility gaps	IAM, logging, compliance monitoring	Misconfiguration events, identity access reviews

Table 29: Cybersecurity Risk Deep Dive

11.2 Supply Chain Risk Assessment

Supply Chain Risk Type	Example Scenarios	Mitigation Strategies	Monitoring Metrics
Supplier Concentration	Single source of critical material; logistics capacity	Diversify suppliers; nearshoring; inventory buffers	Concentration %; alternative sources available
Supplier Financial Viability	Insolvency; inability to meet obligations	Financial health monitoring; contract clauses; escrow	Credit scores; cash positions; contingency plans

Supply Chain Risk Type	Example Scenarios	Mitigation Strategies	Monitoring Metrics
Geopolitical / Trade Quality	Sanctions, trade wars, tariffs, border disruptions	Multi-region sourcing; customs planning; policy monitoring	Trade corridor health, lead times, tariff exposure
Compliance	Defects, recalls, non-compliance with standards	Quality audits, SLAs, corrective action plans	Defect rates, audit findings, on-time delivery

Table 30: Supply Chain Risk Assessment Framework

11.3 Emerging/Horizon Risk Assessment

Use foresight techniques to identify emerging risks on the periphery of awareness.

Emerging Risk	Time Horizon	Source/Trigger	Early Action
Quantum computing	5-10 years	Cryptography vulnerability	Begin crypto-agility roadmap; migrate key systems
AI/ML governance	2-3 years	Regulatory focus; ethical concerns	Establish AI governance framework; skills building
Climate-related transition	2-5 years	Investor pressure; regulation; customer demand	Conduct climate scenario analysis; set net-zero targets
Biosecurity/pandemics	Ongoing	COVID-19 lessons; surveillance gaps	Enhance pandemic preparedness; supply chain resilience
Geopolitical fragmentation	3-5 years	Trade blocs; de-globalisation	Stress-test supply chain; regulatory complexity planning

Table 31: Emerging/Horizon Risk Considerations

Part 12: Templates Summary & Quick-Start Checklist

12.1 Risk Assessment Pack Templates Checklist

Use this checklist to ensure all assessment activities and templates are completed:

- [ ] **Scope & Context Definition** – Documented assessment scope, participants, timeframe
- [ ] **Risk Identification Workshop** – Facilitated session with cross-functional team; risks captured
- [ ] **Risk Identification Register** – All identified risks listed with ID, category, description, causes
- [ ] **Risk Analysis** – Likelihood and Impact assessed for each risk (Inherent and Residual)
- [ ] **Control Assessment** – Existing controls documented and rated for effectiveness
- [ ] **Risk Interdependencies** – Cascading/correlated risks identified and noted
- [ ] **Risk Evaluation** – Residual scores compared to tolerance criteria; evaluation bands assigned
- [ ] **Risk Heat Map** – Visual representation of risk positioning created
- [ ] **Risk Treatment Plans** – Detailed treatment actions defined for Manageable/Unacceptable risks
- [ ] **Master Risk Register** – Consolidated register with all risks, controls, treatments, ownership
- [ ] **KRI Dashboard** – Key risk indicators selected and baselines established
- [ ] **Board/Governance Report** – Executive summary prepared for Board/Audit Committee review
- [ ] **Action Items Log** – All outstanding actions assigned with owner and due date

12.2 Quick-Start Implementation Timeline

Phase	Timeline	Key Activities
Phase 1: Preparation	Week 1-2	Define scope; engage stakeholders; schedule workshops; prepare materials
Phase 2: Identification	Week 3-4	Conduct risk identification workshops; capture risks; consolidate list
Phase 3: Analysis	Week 5-6	Assess likelihood/impact; review controls; create heat map
Phase 4: Evaluation & Treatment	Week 7-8	Evaluate vs. criteria; prioritise; develop treatment plans
Phase 5: Reporting & Approval	Week 9	Prepare governance report; Executive/Board review and approval
Phase 6: Implementation	Week 10+	Commence treatment actions; establish monitoring cadence; ongoing tracking

Table 32: Risk Assessment Implementation Timeline (9-week typical cycle)

Part 13: Supporting Resources & References

13.1 Key Reference Documents

- **ISO 31000:2018** – Risk Management – Principles and Guidelines
- **ISO 31010:2019** – Risk Management – Risk Assessment Techniques
- **IRMSA Guideline: Integrating Strategy, Risk and Resilience** (2022)
- **King V Code of Governance for South Africa** (2025)
- **COSO Enterprise Risk Management – Integrated Framework** (2017)
- **NIST Cybersecurity Framework** (for cyber risk assessment)
- **TCFD Climate-Related Financial Disclosures** (for climate risk assessment)

13.2 Additional Assessment Techniques

Beyond qualitative workshops, consider these techniques for deeper analysis:

- **Red Team / Devil's Advocate Sessions** – Challenge assumptions; surface hidden risks
- **Delphi Technique** – Anonymous expert surveys to build consensus on risk estimates
- **Historical Data Analysis** – Review past incidents, claims, audit findings for patterns
- **Failure Mode & Effects Analysis (FMEA)** – Systematic process risk analysis for critical processes
- **Bow-Tie Analysis** – Visual representation of causes → risk event → consequences
- **Stress Testing & Scenario Analysis** – Test strategy/finances against downside scenarios

13.3 Recommended Risk Management Software Platforms

Common platforms used for risk assessment, tracking and reporting:

- **Archer Risk & Compliance** (industry-leading ERM platform)
- **LogicGate** (mid-market GRC platform)
- **Domo / Tableau** (risk dashboards and KRI tracking)
- **Microsoft 365** (for distributed teams; lightweight tracking)
- **Spreadsheet-based** (Excel with version control; suitable for smaller organisations)

Appendix: Glossary of Terms

Term	Definition
Risk	Effect of uncertainty on objectives (ISO 31000:2018); potential for gain or loss
Risk Category	Classification of risk (e.g. Strategic, Financial, Operational, Compliance, Reputational, Cyber)
Likelihood	Probability or frequency that a risk event will occur
Impact/Consequence	Potential magnitude of effect if risk event occurs; measured in financial, operational, reputational dimensions
Risk Score	Quantitative estimate of risk = Likelihood × Impact
Inherent Risk	Risk exposure without considering existing controls or mitigation actions
Residual Risk	Risk exposure after considering existing controls or mitigations
Control	Action, process, or procedure that reduces risk (likelihood or impact)
Risk Appetite	Willingness of organisation to accept levels and types of risk to achieve strategic objectives
Risk Tolerance	Specific, measurable limits for accepting risk by category, organisation-wide or per business unit
Risk Evaluation	Comparison of risk assessment results against risk criteria to determine treatment priority
Risk Treatment	Actions taken to modify risk (Treat, Transfer, Tolerate, Terminate)
Key Risk Indicator (KRI)	Leading indicator signalling emerging risk before it materialises
Stakeholder	Party with interest in or influenced by organisational risks (e.g. investors, customers, employees, regulators)

Term	Definition
ISO 31000	International standard for risk management principles, framework and process

Table 34: Glossary of Terms

Document Control

Item	Detail
Document Title	ISO 31000:2018 Risk Assessment Pack
Version	1.0
Date Created	
Effective Date	
Document Owner	Chief Risk Officer / Risk & Compliance Function
Classification	Confidential – Internal Use Only
Review Frequency	Annual or when ISO 31000 guidance is updated
Next Review Date	

Approval Sign-Off

Role	Name/Title	Signature/Date
Chief Risk Officer	[Name]	[Date]
Chief Executive Officer	[Name]	[Date]
Board Audit Committee Chair	[Name]	[Date]

Table 35: Document Approval and Sign-Off