MBM VALKYRIE ADVISORY (PTY) LTD
INDEPENDENT LEGAL, GOVERNANCE & COMPLIANCE ADVISORY
Registration No. 2026/493372/07 · CSD MAAA1746312 · B-BBEE Level 1 EME · Not registered for VAT
31 Ouklipmuur Avenue, Equestria, Pretoria, Gauteng, 0184

+27 61 586 9435
enquiry@mbmvalkyrie.co.za
www.mbmvalkyrie.co.za

REFERENCE LIBRARY · MBM-LIB-02 · VERSION 1.0

The policy instrument library

Thirty-eight policy instruments — what each does, how it is drafted, and the defect that most often makes it unenforceable.

Every policy has two audiences: the people who must follow it, and the person who will one day read it against you — a commissioner, an assessor, an auditor, a funder or a regulator. A policy copied from another organisation satisfies the first audience and fails the second, because it describes controls that do not exist here. This library is general guidance and not legal advice on your facts.

Contents

01 · Board and governance policies

The instruments that decide who may decide. They are drafted from the enabling instrument outwards — the Act, then the MOI or constitution, then the board's own resolutions — never from a template inwards.

Delegation of Authority framework

States what the board keeps, what it delegates, to whom, and up to what value — so that every decision in the organisation can be traced to an authority that existed when it was taken.

HOW IT IS DRAFTED

Start with a diagnostic of how decisions are actually taken today, then map that against the enabling Act, the MOI or constitution, the PFMA or MFMA where applicable, and the board's resolutions. Build a tiered matrix from board to committee to chief executive and downwards, with financial thresholds and decision types; an approval workflow; sub-delegation rules; a reservation schedule of matters that may never be delegated; and a review trigger. Close with an implementation guide and a board resolution adopting it.

WHAT TO LOOK OUT FOR

Three failures recur. A framework that delegates powers the enabling Act reserves to the board itself is void, and the decisions taken under it are open to review. Thresholds set in rands that were realistic four years ago are breached routinely and quietly. And a matrix with no sub-delegation rule means an executive's authority evaporates the moment they go on leave.

Board charter and committee terms of reference

Records how the governing body governs itself: composition, powers, meeting discipline and the division of work between the board and its committees.

HOW IT IS DRAFTED

Draft the charter against the Companies Act, the MOI and the applicable King principles: role and responsibilities, composition and independence, appointment and rotation, quorum, conflicts, information rights, evaluation, and the relationship with management. Each committee then gets terms of reference with its own mandate, membership, quorum, meeting frequency, annual work plan and reporting line — audit and risk, remuneration, social and ethics, and nominations.

WHAT TO LOOK OUT FOR

A social and ethics committee is compulsory for state-owned, listed and larger companies, and its functions are prescribed by regulation — a committee whose terms of reference do not track those functions is not performing the statutory function, whatever it is called. And terms of reference granting a committee decision-making power the board has not delegated produce decisions that are open to challenge.

Conflict of interest and declaration of interests policy

Requires interests to be disclosed before they influence a decision, and governs what happens once they are — the single policy most often asked for by auditors, funders and supply-chain offices.

HOW IT IS DRAFTED

Define “interest” widely enough to be useful: direct and indirect financial interests, interests of a related person, directorships and memberships, outside remunerative work, gifts and hospitality, and personal relationships with counterparties. Then build the machinery — an annual written declaration by every director, employee and committee member; a standing agenda item at every meeting; a per-item disclosure duty; a register that is maintained rather than filed; and a clear recusal rule stating whether the conflicted person leaves the room, whether they may answer questions first, and whether they count towards the quorum. For a company, track section 75 of the Companies Act precisely: what must be disclosed, when, and the consequence of failing to. For a public entity, align it with the procurement declaration forms and with the Public Service Regulations where they apply. Provide for the case the policy usually forgets: the sole director, or the chairperson, being the conflicted person.

WHAT TO LOOK OUT FOR

Most conflict policies fail on quorum and on evidence. If the conflicted member recuses but is still counted for quorum, the decision is vulnerable; say expressly how quorum is calculated after recusal and what happens if the remaining members are not quorate. And a declaration signed once on appointment is not a system — the register must be tabled, reviewed and minuted, because the value of the policy is entirely in the record it produces. Watch too for the policy that prohibits conflicts rather than managing them: a blanket prohibition is unenforceable in a small market, and drives disclosure underground, which is precisely the opposite of what the policy is for.

Gifts, hospitality and sponsorship policy

Sets the line between ordinary courtesy and inducement, in a form staff can actually apply at the moment they are offered something.

HOW IT IS DRAFTED

Give a monetary threshold below which a gift may be accepted and above which it must be declined or surrendered; a register with a named custodian; an absolute prohibition on cash and cash equivalents; a rule for gifts offered during a live tender or adjudication; treatment of travel and accommodation paid by a counterparty; and a separate rule for gifts given by the organisation.

WHAT TO LOOK OUT FOR

A threshold expressed only in words (“of nominal value”) is unusable — staff need a number. And the register only works if declining is as easy as accepting: provide a one-line form and a named person to send it to, or nothing gets recorded. Where the organisation deals with organs of state, read the policy together with the Prevention and Combating of Corrupt Activities Act — a gift intended to influence is an offence regardless of the threshold in your policy.

Remuneration policy

Explains how the organisation pays — and how it decides what it pays — in a form that can be put to a shareholder or a funder.

HOW IT IS DRAFTED

Cover the philosophy and the benchmark used; the components of pay and their relative weight; the performance measures behind variable pay and who sets them; the approval path for each level, with the board or remuneration committee reserving executive pay; non-executive fees and how they are approved; and the disclosure the organisation will make.

WHAT TO LOOK OUT FOR

For a company, remuneration of directors for their services as directors requires a special resolution within the preceding two years — a board that has quietly paid fees without one has a recoverable payment on its hands. The Companies Amendment Act 16 of 2024 goes considerably further for public and state-owned companies, requiring a remuneration policy tabled for approval by shareholders and a remuneration report disclosing, among other things, the ratio between the highest and lowest paid employees — so a policy drafted for those companies must now be written to be voted on and published, not merely to be followed. And a policy that promises benchmarking against a peer group nobody has defined will be read against the organisation the first time pay is questioned.

Board evaluation and induction policy

Makes the annual assessment of the governing body a governed process rather than an occasional exercise.

HOW IT IS DRAFTED

State the cycle — self-assessment, peer and chair review, external review at a stated interval; the instrument used; who collates and who sees the raw responses; how findings become an action plan with owners and dates; and how the outcome is reported. Attach the induction pack: founding documents, delegations, charters, the last two years of minutes, the risk register and the current strategy.

WHAT TO LOOK OUT FOR

An evaluation with no confidentiality rule produces bland answers, and an evaluation with no action plan produces nothing at all. Name who receives the individual responses before the first one is collected.

02 · Ethics, conduct and integrity policies

The documents an organisation is judged by when something has gone wrong — and which are worth less than nothing if they describe a system that does not exist.

Code of conduct and ethics

States the standard of behaviour required of everyone who acts in the organisation’s name.

HOW IT IS DRAFTED

Write it in the second person and in specifics, not in values-language: honesty in client communication, competence and the duty to decline work beyond it, independence and objectivity, confidentiality, dealings with regulators and organs of state, use of the organisation’s assets and systems, outside interests and public comment, and responsible corporate citizenship. Attach an annual written acknowledgement, a reporting route for breaches, and the consequence of a breach expressed as a disciplinary matter.

WHAT TO LOOK OUT FOR

A code that only recites values cannot be enforced, because no-one can point to the rule that was broken. And where a member of staff is subject to a professional code as well — an attorney, an accountant, an engineer — say expressly that the stricter standard applies, or the two codes will be argued against each other at exactly the wrong moment.

Whistleblowing and protected disclosures policy

Creates a route by which someone can report wrongdoing without paying for it.

HOW IT IS DRAFTED

Identify what may be disclosed and to whom; provide at least one channel that bypasses line management and one that bypasses the executive entirely; set out how the discloser's identity is protected and what anonymity can and cannot be promised; record the protections against occupational detriment under the Protected Disclosures Act; state the investigation process, the timelines and the feedback the discloser will receive; and provide for false or malicious disclosure.

WHAT TO LOOK OUT FOR

A policy that routes disclosures to line management defeats itself — the channel must bypass the people most likely to be the subject of a disclosure, which is a governance design question before it is a drafting one. Do not promise absolute anonymity you cannot deliver once an investigation or a court process begins; promise confidentiality, and describe its limits honestly. And remember the employer's own duty under the Act to respond to a disclosure within the prescribed period — silence is itself a failure.

Anti-bribery and anti-corruption policy

Prohibits improper payments and, just as importantly, creates the duty to report them.

HOW IT IS DRAFTED

Prohibit bribery in both directions, including through agents and intermediaries; address facilitation payments expressly; require due diligence on intermediaries and a contractual anti-bribery undertaking; govern political and charitable donations; and set out the internal reporting route and the statutory reporting duty.

WHAT TO LOOK OUT FOR

Section 34 of the Prevention and Combating of Corrupt Activities Act places a personal duty on a person in a position of authority to report certain corrupt activities above the prescribed amount to a police official — that duty sits on the individual, not on the organisation, and a policy that does not say so leaves its executives exposed. Facilitation payments are not lawful in South Africa; a policy that treats them as a grey area is a policy that has been copied from another jurisdiction.

Fraud prevention and response plan

Moves the organisation from intention to machinery: what is done to prevent fraud, what happens when it is suspected, and who decides.

HOW IT IS DRAFTED

Set out the fraud risk assessment and its cycle; the preventive controls mapped to the risks; detection routes including the whistleblowing channel and data analytics; the response protocol — who is told, who secures evidence, who suspends, who investigates and who may not; the decision on criminal and civil recovery and who takes it; and the reporting to the audit and risk committee.

WHAT TO LOOK OUT FOR

The response protocol is the part that is always thin and always needed at speed. Name the roles now, because deciding who leads an investigation while it is running is how evidence is lost and how a subsequent dismissal becomes procedurally unfair.

Client acceptance, engagement and independence policy

Decides which work the organisation will take, from whom, and on what terms — before capacity and cash flow decide it instead.

HOW IT IS DRAFTED

Cover the conflict search and how it is recorded; competence and capacity screening; the risk rating of a prospective client; customer due diligence where the FIC Act applies; the engagement letter as the only basis on which work starts; independence safeguards and the circumstances requiring declinature; fee and payment terms; and the file-closure and retention rule.

WHAT TO LOOK OUT FOR

An acceptance policy without a declinature route is decorative. Write down what the organisation will not take and who may say no, and make the conflict search a step that produces a record, because the record is what you will be asked for.

03 · Finance, procurement and asset policies

Where the policy is the control. In the public sector these are prescribed rather than optional, and the drafting question is compliance before preference.

Financial management policy

Governs how money moves: budgeting, authorisation, payment, recording and reporting.

HOW IT IS DRAFTED

Address the budget cycle and who approves it; the chart of accounts and the accounting framework applied; banking mandates and dual authorisation with thresholds; the separation of the person who requests, the person who approves and the person who pays; petty cash; credit control and write-offs; month-end and year-end procedures; the audit or independent review arrangement; and tax compliance.

WHAT TO LOOK OUT FOR

The control that fails most often in a small organisation is separation of duties, because there are not enough people — say so honestly and put a compensating control in writing, such as an independent monthly review of the bank statement by someone outside the payment chain. A policy that pretends to a segregation the organisation cannot staff is evidence against it.

Supply chain management and procurement policy

States how the organisation buys — thresholds, methods, committees and the record each produces.

HOW IT IS DRAFTED

Set the procurement thresholds and the method for each band; the composition and quorum of the specification, evaluation and adjudication committees, and who may not sit on them; the declaration of interest at each stage; evaluation criteria published in advance and applied as published; deviation and confinement rules with written reasons; contract management after award; and the supplier database and its screening.

WHAT TO LOOK OUT FOR

For a municipality the policy itself is a statutory requirement under section 111 of the MFMA, and councillors may not sit on bid committees. In the national and provincial sphere, the preference regime under the Preferential Procurement Policy Framework Act and its current regulations must be applied as the regulations stand rather than as the organisation would prefer — a preference point system applied outside the regulations produces an award that can be set aside. And every deviation must carry contemporaneous written reasons: reasons composed afterwards are where irregular expenditure findings begin.

Irregular, fruitless and wasteful expenditure policy

Tells a public entity what to do the moment expenditure is identified as irregular — which is a different question from how it happened.

HOW IT IS DRAFTED

Define each category in the statutory terms; require immediate recording in the register on identification; set the investigation and determination process; state who decides on recovery, condonation or write-off and on what authority; and set the reporting path to the accounting authority, the executive authority, the Auditor-General and National or Provincial Treasury.

WHAT TO LOOK OUT FOR

Irregular expenditure is not automatically a loss and not automatically recoverable, and conflating the two paralyses the process. The register must be opened on identification rather than on conclusion of the investigation — a register written up at year end is the finding. Note also the material irregularity regime under the Public Audit Act: once the Auditor-General notifies one, the accounting officer's response is time-bound.

Asset management policy

Keeps the asset register real, and the assets accounted for.

HOW IT IS DRAFTED

Cover capitalisation thresholds and classification; the asset register and its reconciliation to the financial statements; acquisition and disposal authority; the annual verification count and who performs it; depreciation and impairment; insurance; and the treatment of assets allocated to individuals, including devices.

WHAT TO LOOK OUT FOR

The verification count is the clause that gets skipped, and it is the one an auditor tests. Name the month, name the person, and require an exception report — a register that has never been counted against the floor is an estimate.

Travel, subsistence and expense policy

Sets what may be claimed, at what rate and with what proof.

HOW IT IS DRAFTED

State the approval required before travel; class of travel and accommodation caps; the subsistence basis — actual with receipts or a daily allowance within the SARS-published limits; the mileage rate used; the claim form, deadline and supporting documents; and the consequence of a late or unsubstantiated claim.

WHAT TO LOOK OUT FOR

Tie the subsistence and mileage rates to the SARS-published figures by reference rather than by number, or the policy is out of date every March and the difference becomes a fringe benefit somebody has to account for.

Credit control, debt and write-off policy

Governs what the organisation does when it is not paid.

HOW IT IS DRAFTED

Set the credit assessment before terms are granted; the terms themselves; the escalation calendar — reminder, letter of demand, handover; who may agree a payment arrangement and on what terms; the criteria and authority for write-off; and the prescription check before handover.

WHAT TO LOOK OUT FOR

Check prescription before every handover: three years from the debt becoming due, and an acknowledgement of liability restarts the clock. Handing a prescribed debt to a collection agency is at best wasted money and at worst a complaint.

04 · Information, data and records policies

The suite the Information Regulator asks for — and which, for an organisation that sells compliance, is the first thing a sceptical buyer checks.

Information governance and POPIA policy

Records how the organisation processes personal information, and by what lawful basis.

HOW IT IS DRAFTED

Build it on an inventory and data-flow map, not on a template: what personal information is held, where it lives, who touches it and why. Then state the lawful basis for each purpose against the eight conditions; the roles of the Information Officer and deputies and their registration; the rights of data subjects and how requests are handled; the operator register and the agreements behind it; special personal information and children's information; direct marketing; cross-border transfers; security safeguards; retention; and the training cycle.

WHAT TO LOOK OUT FOR

The operator register is almost always the real gap — the clause is easy, identifying every third party that touches personal information is not. Start with the payroll bureau, the cloud host, the marketing agency, the shredding company and the IT support firm. And consent is the lawful basis organisations reach for first and can rely on least: it must be voluntary, specific and informed, and it can be withdrawn, which makes it the weakest foundation for processing the business depends on.

PAIA manual and access to information procedure

The public document section 51 of PAIA requires, plus the internal procedure that makes it answerable.

HOW IT IS DRAFTED

The manual must give the particulars of the body and its information officer, a description of the records held by subject and category, the records available without a request, the request procedure and forms, the fees, and the remedies available to a requester. Behind it, an internal procedure: who receives a request, the decision-maker, the statutory time limits, third-party notification, and the form of the decision with reasons.

WHAT TO LOOK OUT FOR

The section 51 manual is the cheapest credibility signal available: it is public, it is compulsory, and its absence is the first thing a complainant points at. Keep it current — a manual naming an information officer who left is worse than none, because it proves the obligation was known and then abandoned.

Records management and retention policy

Says how long each class of record is kept, where, and how it is destroyed.

HOW IT IS DRAFTED

Build a retention schedule by record class, each line carrying its legal basis — the Companies Act seven-year rule for company records, tax records under the Tax Administration Act, employment records under the BCEA and the Employment Equity Act, occupational health records, and the POPIA principle that personal information is not kept longer than necessary. Add the storage medium, the custodian, the destruction method and the destruction certificate, and a litigation hold that suspends destruction.

WHAT TO LOOK OUT FOR

POPIA pulls in the opposite direction from the instinct to keep everything, and both directions are enforceable — which is why each line needs its own legal basis rather than a single global period. And the litigation hold is the clause that saves the organisation: routine destruction of records after a dispute has become foreseeable is very hard to explain.

Information security and acceptable use policy

Describes the technical and organisational measures that make the POPIA security condition real, and what staff may and may not do with the organisation's systems.

HOW IT IS DRAFTED

Cover access control and the joiner-mover-leaver process; passwords and multi-factor authentication; device and removable-media rules; encryption in transit and at rest; email and internet use; personal device use and what the organisation may do with a personal device it has enrolled; remote access; patching and backup with a tested restore; third-party and cloud service approval; and monitoring, with notice of monitoring given in advance.

WHAT TO LOOK OUT FOR

Monitoring without prior notice is where an otherwise sound policy becomes evidence against the employer — interception and monitoring of communications must be dealt with squarely and disclosed before it happens. And a backup that has never been restored is not a backup: require a documented test restore at a stated interval, because that is the line an assessor will ask you to prove.

Security compromise and data breach response procedure

The operational procedure for the day personal information is exposed.

HOW IT IS DRAFTED

Define what counts as a security compromise and how it is reported internally; the containment steps and who takes them; the assessment of risk to data subjects; the notification to the Information Regulator and to affected data subjects, with templates drafted in advance; the record of the incident; and the post-incident review.

WHAT TO LOOK OUT FOR

POPIA requires notification as soon as reasonably possible after discovery, and the recent enforcement pattern is that reporting an incident invites an assessment of the processing behind it — so the procedure must assume that the Regulator will look past the incident. Draft the notification templates now, in calm conditions; nobody drafts well on the day.

Communications, media and social media policy

Governs who may speak for the organisation, and what everyone else may say.

HOW IT IS DRAFTED

Name the authorised spokespersons and the escalation route for media enquiries; separate official channels from personal accounts; set rules on confidential information, client identification and sub judice matters; deal with endorsements and paid content disclosure; and state the review and approval path for published material.

WHAT TO LOOK OUT FOR

The clause that matters is the personal-account clause, and it must be proportionate: an employer may regulate speech that identifies the employer or discloses its information, but a policy reaching into private expression generally will not survive a challenge. Draft to the connection with the workplace, not to the sentiment.

05 · People and workplace policies

Employment policies are read twice: once by the employee, and once by a commissioner deciding whether the employer followed its own rules.

Disciplinary code and procedure

Sets out the standards of conduct, the process for addressing a breach, and the sanctions available.

HOW IT IS DRAFTED

Align it to Schedule 8 of the Labour Relations Act: the distinction between misconduct, incapacity and operational requirements; a non-exhaustive list of offences with indicative rather than fixed sanctions; progressive discipline; the investigation; the notice of hearing and its contents; the right to representation and the limits on it; the presiding officer and their independence; the record of the hearing; the ruling with reasons; and appeal or review.

WHAT TO LOOK OUT FOR

A code that reads as a rigid tariff of sanctions removes the discretion the employer needs, and is then used against the employer at the CCMA — keep it a guide, and say so. The most common reason an employer loses is not the substance but the record: charges drafted too narrowly to cover what the evidence proved, or a ruling that states a conclusion without the reasoning that supports it.

Grievance procedure

Gives employees a route to raise a complaint that does not require them to resign first.

HOW IT IS DRAFTED

Provide informal resolution before the formal steps; a form and a named recipient; timelines at each stage; an alternative route where the grievance concerns the line manager; the right to be accompanied; the outcome in writing with reasons; and escalation.

WHAT TO LOOK OUT FOR

An alternative route around the line manager is the whole point of the procedure — without it, the grievances that matter most are the ones that never get filed.

Harassment and sexual harassment policy

Prohibits harassment in all its forms and sets out how a complaint is handled.

HOW IT IS DRAFTED

Follow the Code of Good Practice on the Prevention and Elimination of Harassment in the Workplace: define harassment broadly, including sexual harassment, racial, ethnic and social-origin harassment, and bullying; describe both the informal and the formal procedure; provide for the complainant's choice between them; set out confidentiality, support and protection against victimisation; identify trained persons who may receive a complaint, of more than one gender; and address third parties — clients, suppliers and visitors.

WHAT TO LOOK OUT FOR

The Code expects every employer to adopt a harassment policy and to communicate it, and an employer that fails to take reasonable steps once it knows of harassment can be held liable under the Employment Equity Act. Two drafting points decide whether the policy works: the complainant must be able to choose the informal route without losing the formal one, and the person receiving complaints must not be the employee's own manager.

Recruitment, selection and appointment policy

Makes hiring a governed process with a record, rather than a conversation with an outcome.

HOW IT IS DRAFTED

Cover the authority to create and fill a post; the job profile and the inherent requirements of the job; advertising; shortlisting criteria set before applications are read; the panel and its composition; interview record-keeping; verification of qualifications, criminal and credit checks where lawful and job-related; reference checks; the offer and its approval; and the appointment record.

WHAT TO LOOK OUT FOR

Criminal and credit checks must be job-related, and credit checks in particular are constrained — a blanket policy of checking everybody is difficult to defend. Set shortlisting criteria before the applications are opened; criteria written afterwards are indistinguishable from a preference, and that is exactly how an unsuccessful candidate will describe them.

Employment equity and diversity policy

Connects the organisation's employment practices to its equity plan and its statutory reporting.

HOW IT IS DRAFTED

Record the consultative forum and its composition; the analysis of the workforce profile and of employment barriers; the numerical goals and the plan behind them; affirmative-action measures; reasonable accommodation; the income-differential review; the assignment of a senior manager to the function; and the reporting calendar.

WHAT TO LOOK OUT FOR

The amended Employment Equity Act brings sector numerical targets and ties a compliance certificate to state contracting — an organisation that tenders and cannot show compliance is not merely non-compliant, it is ineligible. Check which obligations attach at the organisation's headcount and turnover before drafting, since designated-employer status changes the whole document.

Leave and attendance policy

States each kind of leave, how it is applied for and what proof is required.

HOW IT IS DRAFTED

Cover annual, sick, family responsibility, maternity, parental, adoption and commissioning parental leave, each at or above the BCEA minimum; the leave cycle and forfeiture rules; medical certificate requirements and the two-day rule; unpaid leave; study leave; and the record kept.

WHAT TO LOOK OUT FOR

The BCEA is a floor, not a menu. A policy granting less — a shorter sick-leave cycle, a forfeiture rule that defeats the statutory minimum — is void to that extent, and the organisation will be held to the Act while its staff have been told something else. Parental leave provisions have been the subject of litigation and legislative change; check the current position rather than copying last year's policy.

Performance management and incapacity policy

Makes poor performance a managed process with a fair outcome, rather than a dismissal waiting to be reversed.

HOW IT IS DRAFTED

Set the performance cycle, the standards and how they are communicated; regular review and its record; the formal performance improvement process — the standard, the assistance, the period and the consequence; the incapacity procedure for ill health, including the duty to investigate alternatives and to accommodate; and the distinction between poor performance and misconduct.

WHAT TO LOOK OUT FOR

Schedule 8 requires evaluation, instruction, training, guidance or counselling and a reasonable opportunity to improve before dismissal for poor performance — a policy that goes straight to a final warning skips the part that decides the case. Ill-health incapacity is not misconduct and must never be routed through the disciplinary code.

Remote and hybrid work policy

Governs work done away from the employer's premises.

HOW IT IS DRAFTED

Cover eligibility and the approval process; hours, availability and the right to be unavailable; equipment, data costs and who bears them; the home workstation and the employer's health and safety duty; information security and the acceptable-use overlap; supervision and performance measurement; and the notice required to change or end the arrangement.

WHAT TO LOOK OUT FOR

Health and safety duties do not stop at the office door, and neither does POPIA — a household printer and an unlocked laptop are a processing risk the employer remains responsible for. If remote work has been in place long enough to have become a term of employment, changing it unilaterally is a change to terms and conditions, not a management instruction.

Occupational health and safety policy

The written statement of the employer's health and safety commitment, and the machinery behind it.

HOW IT IS DRAFTED

State the general duty and the specific arrangements; the section 16(2) assignment of responsibility in writing; health and safety representatives and the committee where the headcount requires them; risk assessment and its cycle; incident reporting and investigation; emergency and evacuation procedures; first aid; contractor and visitor duties; and COIDA registration and claims.

WHAT TO LOOK OUT FOR

The section 16(2) assignment must exist in writing and name a person — without it, the duty stays with the chief executive personally. And the policy must match the actual premises: an evacuation procedure describing a building the organisation left two years ago is the version that will be produced after an incident.

06 · Risk, compliance and operational policies

The policies that decide whether the organisation notices a problem early enough to do something about it.

Risk management policy and framework

Sets the organisation's risk appetite and the process by which risks are identified, rated, treated and reported.

HOW IT IS DRAFTED

Cover governance of risk and the board's role; the risk appetite and tolerance statement; the methodology — categories, likelihood and impact scales, inherent and residual rating; the risk register and its owner; the treatment options and the control owner for each; the assurance map; the reporting cycle to the audit and risk committee; and emerging-risk review.

WHAT TO LOOK OUT FOR

A risk register with no named control owner and no review date is a list, not a control. And an appetite statement that says the organisation has no appetite for any risk tells the board nothing and licenses everything — express appetite differently for different categories.

Compliance policy and regulatory universe

Identifies every statute and regulator that binds the organisation, and who owns each obligation.

HOW IT IS DRAFTED

Build the regulatory universe first: each Act and subordinate instrument, the obligations it creates, the owner, the control, the evidence and the frequency. Then the policy around it — how the universe is maintained, how legislative change is monitored, the compliance calendar, breach reporting and remediation, and reporting to the board.

WHAT TO LOOK OUT FOR

The perimeter question is usually answered by the product roadmap rather than the current product — a feature six months away can bring an entire licensing regime with it, and the time to know is before it is built. A universe that lists statutes without naming an owner for each obligation cannot be used, and will not be.

FIC Act Risk Management and Compliance Programme

The programme every accountable institution must have, in the form the FIC Act prescribes.

HOW IT IS DRAFTED

Document the risk-based approach and the risk rating methodology; customer due diligence, including identification and verification, beneficial ownership and ongoing due diligence; enhanced measures for domestic and foreign prominent influential persons; sanctions and targeted financial sanctions screening; record-keeping; the reporting workflow for cash threshold, suspicious and terrorist property reports; the compliance officer's appointment; training; and independent review.

WHAT TO LOOK OUT FOR

A programme bought as a template and never operationalised is worse than none: it is documentary proof of what the institution said it would do and did not. The FIC's inspections test the doing — the training register, the screening records, the reports actually filed — not the document.

Business continuity and disaster recovery policy

States what the organisation will do to keep operating, and how quickly.

HOW IT IS DRAFTED

Identify the critical functions and their dependencies through a business impact analysis; set recovery time and recovery point objectives per function; describe the arrangements — alternate site, remote working, backup and restore, key supplier alternatives; define invocation authority and the crisis team; set the communication plan for staff, clients and regulators; and require a testing cycle with a written report.

WHAT TO LOOK OUT FOR

Recovery objectives that have never been tested against the actual backup are aspirations. Test the restore, write down how long it took, and change the objective if the answer is inconvenient — an untested four-hour objective is worse than an honest two-day one.

Complaints management policy

Turns a complaint into a record and a response rather than a grievance that escalates elsewhere.

HOW IT IS DRAFTED

Define what counts as a complaint; provide accessible channels; set acknowledgement and resolution timelines; identify the decision-maker and an escalation route independent of the person complained about; require a register with root-cause analysis; state the external remedies available, including the relevant ombud or regulator; and report trends to the board.

WHAT TO LOOK OUT FOR

Telling complainants about the external remedy is not a weakness — for many regulated sectors it is a requirement, and an organisation that conceals it converts a complaint into a regulatory matter. The register is the asset: three complaints about the same clause is a drafting problem, not a service problem.

Third-party, outsourcing and vendor management policy

Governs the risk the organisation takes on when it lets someone else do the work.

HOW IT IS DRAFTED

Cover the pre-contract due diligence and its risk tiers; mandatory contract terms including audit rights, security, POPIA operator terms, sub-contracting consent and exit assistance; performance monitoring against service levels; the vendor register; concentration risk; and the offboarding procedure including return or deletion of data.

WHAT TO LOOK OUT FOR

Responsibility cannot be outsourced, only the activity. Where the vendor processes personal information the organisation remains the responsible party under POPIA, and where the vendor performs a regulated function the regulator still holds the organisation. Draft the exit provisions at the start — they are impossible to negotiate at the end.

The seven disciplines behind every policy

Anchor it to the source. Every policy should name the Act, regulation, code or founding-document provision it gives effect to, in its own opening. A policy that cannot say why it exists cannot be defended, and cannot be updated when the source changes.

Write for the person who must obey it. Policies are applied by people under pressure. Short sentences, the second person, a number instead of “reasonable”, and a named role instead of “the relevant manager”.

Build the machinery, not just the rule. The rule is the easy half. The register, the form, the named custodian, the standing agenda item and the review date are what convert a statement of intent into evidence.

Give it an owner and a review date. Every policy carries document control: reference, owner, approver, version, effective date and next review. An undated policy with no owner is treated by an auditor as not in force.

Adopt it properly. A policy takes effect when the body with authority adopts it. Record the resolution, the date and the authority relied on, and keep the adopted version — not the working draft — as the official copy.

Communicate it, and prove that you did. Acknowledgement records, training registers and intranet publication dates are what answer the question “did your staff know?”. That question is asked in every disciplinary and every assessment.

Review on a trigger as well as a cycle. An annual cycle is not enough. Legislative amendment, an incident, a finding, a restructure or a new product should each trigger a review of the affected policies.

Company information

Registered name	MBM Valkyrie Advisory (Pty) Ltd
Registration number	2026/493372/07
Registered address	31 Ouklipmuur Avenue, Equestria, Pretoria, Gauteng, 0184
Telephone	+27 61 586 9435
Email	enquiry@mbmvalkyrie.co.za · brianm@mbmvalkyrie.co.za
Website	www.mbmvalkyrie.co.za
Director	Mthokozisi Brian Mhlongo (LLB) — admitted attorney of the High Court of South Africa (Gauteng Division, Pretoria), enrolled with the Legal Practice Council on the roll of non-practising legal practitioners
CSD supplier number	MAAA1746312
B-BBEE status	Level 1 EME — sworn affidavit, valid to 22 June 2027
Tax	Tax compliant. Not registered for VAT — no VAT is charged
Professional indemnity	R5 000 000 — iTOO Special Risks
PAIA	Section 51 manual published at www.mbmvalkyrie.co.za/paia-manual

MBM Valkyrie Advisory (Pty) Ltd is an independent advisory company. It is not a firm of attorneys, does not conduct a legal practice for its own account, holds no trust account and does not undertake reserved legal work. Its director is an admitted attorney enrolled with the Legal Practice Council on the roll of non-practising legal practitioners.

How to use this document

Every entry in this library is also published, with its own web address, at **www.mbmvalkyrie.co.za** — so an email or a post can link to a single instrument rather than to a page the reader has to search. If one of these is in front of you now, a thirty-minute scoping call is free: **www.mbmvalkyrie.co.za/book-a-call**, **enquiry@mbmvalkyrie.co.za** or **+27 61 586 9435**. A fixed-fee review of a contract or policy you did not draft, with written advice, is R3 500.