Compliance Management Policy and Operating Procedure Manual

<table>
<tr><td rowspan="3">  </td><td rowspan="3">EDUCATION LABOUR RELATIONS COUNCIL</td><td colspan="2">Doc No. IA/COD&E/005</td></tr>
<tr><td>Date: MAY 2016</td><td>Rev 0</td></tr>
<tr><td colspan="2">Page: 2 of 31</td></tr>
<tr><td colspan="3">Title: COMPLIANCE MANAGEMENT POLICY AND OPERATING PROCEDURE MANUAL</td><td>Document type:
POLICY</td></tr>
<tr><td colspan="3">This document has been seen and accepted by the following:
EXECUTIVE COMMITTEE OF THE COUNCIL</td><td>COMPILED/ REVIEWED BY:

NELISIWE BONGCO
INTERNAL AUDITOR</td></tr>
<tr><td>RECOMMENDED BY:

NTHABISENG SHADUNG
ACTING CHIEF FINANCIAL OFFICER</td><td colspan="2">APPROVED BY:

NOLUSINDISO FOCA
GENERAL SECRETARY</td><td>AUTHORISED BY:

LUVUYO BONO
CHAIRPERSON OF THE COUNCIL</td></tr>
<tr><td colspan="4">DATE OF LAST REVIEW: MAY 2016</td></tr>
<tr><td colspan="4">DATE OF NEXT REVIEW: MAY 2018
NOTE: - This document may be changed before the stipulated period as and when a need arises as guided by the Documentation Policy.</td></tr>
</table>

TABLE OF CONTENTS

DEFINITIONS

For purpose of this policy, unless otherwise stated, the following definitions shall apply:

Code: a mandatory or voluntary statement of recommended practice developed internally by ELRC or externally by an international, national or industry body or other organisation with which the ELRC has chosen to comply with.

Compliance: the act of adhering to and demonstrating adherence to laws, regulations or policies, organisational standards, codes, principles of good governance and accepted ethical standards. This definition includes compliance with:

- The Labour Relations Act
- The ELRC constitution

All other legislative statutes applicable to the ELRC, and all internal policies and procedures, including ELRC's Code of Conduct and Ethics.

Compliance risk: the current and prospective risk of damage to the organisation's business model or objectives, reputation and financial soundness arising from non-adherence with regulatory requirements and expectations of key stakeholders. Compliance risk consists of regulatory and reputational elements.

Regulatory risk: the risk that a business does not comply with regulatory requirements or excludes provisions of relevant regulatory requirements from its operational procedures.

Reputational risk: the risk that the business might be exposed to negative publicity due to the contravention of applicable regulatory requirements.

Compliance assurance: describes the range of activities undertaken to ensure that the standards and requirements set in laws, regulations or policies, standards, codes, principles of good governance and accepted ethical standards are met. These include proactive compliance assurance activities such as education, monitoring, audit and record keeping; and reactive activities such as investigation and enforcement, which occur after any non-compliance has been detected.

Compliance breach or failure: an act or omission whereby any part of the ELRC has not met its compliance obligations, processes or behavioural obligations.

Compliance culture: the values, ethics and beliefs that exist in the ELRC and interact with the ELRC's structures and control systems to produce behavioural norms that are conducive to compliance outcomes.

Compliance management framework: a mechanism through which the ELRC can monitor, review and comply with legislation, regulations, statutes, codes, standards, policies and procedures.

Compliance checklist: a pre-formatted document containing instructions for data entry to monitor compliance with a particular Act, policy, procedure manual, standard and code. Checklists also ensure proper recordkeeping.

Institutional compliance: includes issues of governance, internal structure and decision making processes, principles of procurement, principles of corporate social responsibility, disclosure policies, sustainability reporting and adherence to internal instructions.

Obligation: the laws, regulations, statutes, codes, policies, procedures and community standards with which the ELRC should comply.

Operational compliance: includes the assessment of integrity risk and reputation risk.

1. INTRODUCTION

1.1 The Compliance Management policy and operating procedure is a key component of Compliance Management and articulates how the Compliance Management policy is to be implemented, how compliance management processes are to be carried out and the associated accountabilities for carrying out each stage of the process.

1.2 The Compliance Management policy and procedure manual components are as follows:

Forms and templates

- Annual Compliance Plan
- Non-compliance reporting form
- Register for Non-compliance / breach incidents
- Communication plan Template

Criteria & process flows

- Compliance management process
- Non-compliance/breach assessment criteria
- Non-compliance/breach reporting process

Systems and tools

- Compliance management software/manual

2. VISION AND MISSION

Vision
To improve the quality of teaching and learning through labour peace.

Mission
Quality services for excellence in teaching.

3. COMPLIANCE MANAGEMENT PROCESS

3.1 Understand the Legal and Regulatory Environment (What do we do that might be subject to compliance?)

Most compliance requirements arise from the specific sector within which the ELRC operates, hence it is essential to understand the operations and activities of the ELRC business areas that might be subject to compliance, and where that compliance originates from in order to manage all obligations effectively.

3.1.1 Understand the business environment

Management should understand the business environment they operate in and thus the processes, systems, assets, people, or industry affiliations within their area of responsibility that are subject to compliance requirements.

Since the ELRC is a bargaining council, it has additional compliance requirements imposed by law.

The relevant legislator, regulator or administrator for each compliance requirement should be documented in the centrally held Compliance Register (**Attachment A**)

3.1.2 Determine categories of compliance and maintain the compliance risk universe

Once the business, legislative and regulatory environments have been identified and is understood, the categories of compliance should be determined based on the activities in the ELRC subject to compliance, and hence the risk of non-compliance. These categories of compliance are also what is known as the Compliance Risk Universe, and represent the sources of risk of non-compliance facing the ELRC.

The compliance risk universe incorporates both Regulatory and Business compliance requirements.

The key purposes of the Compliance Risk Universe are as follows:

- Use as a basis for compliance risk assessments;
- To prioritise allocation or resources for managing compliance; and
- Identify areas of responsibility and enable allocation of responsibility to business units.

The Compliance Risk Universe is dynamic and will evolve over time as new compliance requirements are identified and others cease to exist. To support this evolution, the Compliance Risk Universe should be reviewed on an annual basis to incorporate any emerging areas of compliance risk or any areas that are no longer a focus for the ELRC.

3.1.3 Extract of Regulatory Compliance Risk Universe

Act Name	Category	Likelihood	Impact	Result	Indicator
Administrative Adjudication of Road Traffic Offences Act, No. 46 of 1998	Secondary	Minimum	Significant	2	Low Risk (2)
Basic Conditions of Employment Act, No. 75 of 1997	Secondary	Minimum	Major	3	Low Risk (3)
Compensation for Occupational Injuries and Diseases Act, No. 130 of 1993	Secondary	Minimum	Significant	2	Low Risk (2)
Constitution of the Republic of South Africa, No. 108 of 1996	Secondary	Low	Significant	4	Low Risk (4)
Criminal Procedure Act, No. 51 of 1977	Secondary	Minimum	Significant	2	Low Risk (2)
Employment Equity Act, No. 55 of 1998	Secondary	Low	Critical	8	Medium Risk (8)
Labour Relations Act, No. 66 of 1995	Core	High	Critical	16	High Risk (16)

3.1.4 Extract of Business Compliance Universe

#	Custodian: Programme / Sub-Programme	#	Applicable Policies; Laws and Regulations
1	Chief Financial Officer	1	Fraud Prevention Plan
2	Dispute Resolution Services	1	ELRC Constitution
3	Collective Bargaining Services	1	ELRC Constitution
		2	Committee Work Procedures
4	Corporate Service	1	Information Technology Hardware and Software Policy
		2	Disaster Recover Plan
		3	Business Continuity Plan

In order to be able to mitigate the risk of non-compliance and appropriately prioritise and allocate resources to manage compliance, there needs to be knowledge and understanding of the specific compliance requirements and obligations to which the ELRC must adhere to.

3.2 Identify Compliance Requirements

A compliance requirement is a law, (legislated or common law), regulation, government directive, industry code or standard, permit, licence contract or internal policy/procedure that an organisation must comply with.

Compliance requirements can either be:

- Regulatory (legal, licence, contractual, permit or accreditation standards) compliance requirements;
- Business (Internal Policy or “best practice” standards) compliance requirements; or
- Strategic (Corporate Governance practises, King III).

Compliance requirements can be identified through:

- Regular communication with the legislators and regulators;

- Communication with industry bodies;
- Professional associations and memberships;
- Knowledge of the business and operating environment; and
- Internal communication.

3.3 Compliance Register

All compliance requirements are documented in a central Compliance Register which is overseen by Internal Audit. To ensure this register remains up to date, divisional managers are responsible for ensuring any new requirements or changes to existing requirements are communicated to Internal Audit, as and when they occur.

The requirements register will be used to populate the Annual Compliance Plan (**Attachment B**) which describes the annual compliance responsibilities and activities for each Business Unit/Department or Programme.

- Prioritise requirements;
- Identify and manage changes to requirements and obligations.

3.4 Compliance Risk Assessment (Where are we at risk of non-compliance?)

- Identify compliance risks;
- Analyse compliance risks to determine likelihood, consequence or impact and controls; and
- Evaluate compliance risks to determine risk treatment based on analysis.

3.5 Manage Obligations (How do we ensure that we comply?)

- Annual compliance plans;
- Breach reporting and management; and
- Records management.

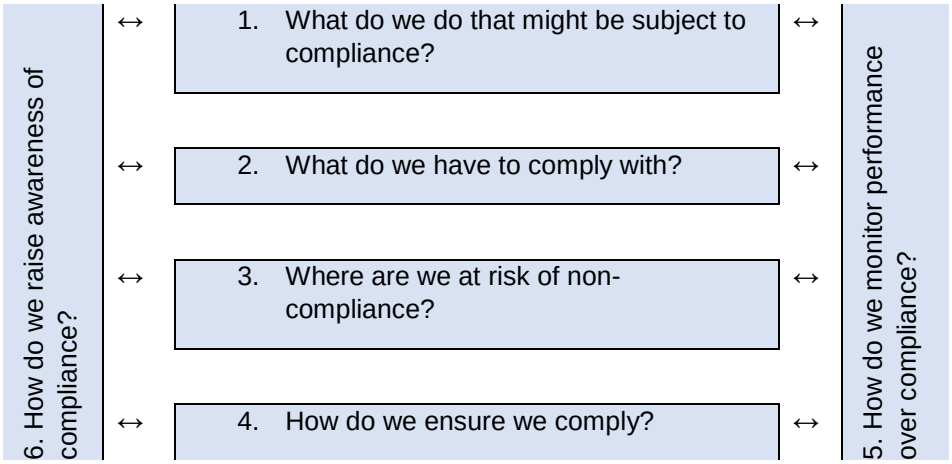
3.6 Monitoring and Evaluation (How do we monitor performance over compliance?)

- Performance measures and metrics;
- Assurance activities; and
- Continuous improvement.

3.7 Communication and Reporting (How do we raise awareness of compliance?)

- Communication;
- Training and education;
- Internal and external reporting; and
- Breach management and reporting.

In simple terms the process can be described by the following questions:



Accountabilities:

Ref.	Accountabilities
Business Unit Manager	
(a)	Understanding processes, systems, or industry affiliations within their area of responsibility that are subject to compliance requirements.
(b)	Understanding of the regulators, legislators and government bodies which monitor or administer the compliance requirements in their area of responsibility.
(c)	Identifying changes to the Compliance Risk Universe and communicating these to Internal Audit.
Internal Auditor	
(d)	Centrally maintaining an up to date Compliance Risk Universe and ensuring it is accessible to all Managers.

4. IDENTIFY COMPLIANCE OBLIGATIONS

A compliance obligation is the specific action within a requirement that an organisation must undertake in order to comply with the overarching compliance requirement.

For example; an obligation with the best practice tools requires the General Secretary to take effective and appropriate steps to prevent unauthorised, irregular and fruitless and wasteful expenditure and losses.

4.1 Compliance Obligations Registers (Attachment B)

Senior Managers are responsible for identifying, documenting and understanding the key obligations under each of the compliance requirements for which they have primary responsibility. These obligations are documented in an Obligations Register.

The obligations register details the following:

- the name of the compliance requirement from which the obligation emanates;
- the obligation itself;
- responsibility for management;
- business units and processes impacted by the obligation;
- the related policy and procedure documents addressing the obligation; and
- the associated ELRC activity (assurance activity) ensuring compliance with the obligation.

The Obligations Register also separately highlights obligations for reporting non-compliance. Refer to the template in **Attachment B** for the format of the Obligations Register

The Obligations Register will identify areas of ELRC which have secondary responsibility for the compliance requirement, i.e. where one or more obligations affect the processes of a business unit/department, so they have responsibility for ensuring compliance with these objectives within their business area, but they are not primarily responsible from a whole organisational perspective. However, these business units are responsible for complying with those obligations whilst carrying out the operations in their area.

The business unit/department that has primary responsibility for a compliance requirement is responsible for ensuring that all business units or areas with secondary responsibilities are aware of the obligations relevant to their activities.

4.2 Compliance Responsibility Map (Attachment C)

Compliance Responsibility Maps table all the business units/departments across the ELRC where a particular compliance requirement has an impact on activities, i.e. the areas in the ELRC where the primary and secondary compliance responsibilities lie. This ensures that the ELRC's points of contact for all compliance requirements are known and understood.

Compliance Responsibility Maps should be compiled for all Level 1 and 2 priority (see 3.3 below) compliance requirements and should be completed and maintained by the business unit that has primary responsibility for the requirement.

Obligation Registers and Responsibility Maps should be updated on an ongoing basis as and when changes occur. A copy of the completed documents should be filed with the Internal Audit department.

4.3 Prioritisation of Compliance Requirements

Once the obligations within a compliance requirement are understood, the relative significance of the requirement to the ELRC should be ascertained and a priority rating assigned, which prescribes the level of ongoing management in accordance with this Policy that the requirement will need.

Prioritising compliance requirements to determine the level of implementation or ongoing management is a subjective process as compliance requirements and their application to the ELRC can vary in nature significantly. Requirements should be assigned a priority level ranging from 1 – 3, with level 1 being the highest priority.

When ranking compliance requirements, the following should be considered:

- Penalties for non-compliance;
- Level of regulation (Administering Body);
- Pervasiveness of compliance requirements across the ELRC;
- Complexity of the compliance requirement;
- Current level of understanding of the requirement;
- Current controls in place for the requirement; and
- Whether the requirement is a regulatory or business requirement.

All rankings must be agreed to with the Internal Auditor.

Approved priority ratings should be documented in the Compliance Requirements and Obligations Registers and the Annual Compliance Plan for the Business Unit.

Priority Level	Application of Compliance Management Policy
1	Compliance Management policy must be implemented in full.
2	Responsibility for the compliance requirement must be included in the Business Unit's Annual Compliance Plan and an Obligations register must be completed. However, implementation of the other elements of the Compliance Management Policy is at the discretion of the Senior Management.
3	The Compliance Management Policy need not be implemented in full, however, the requirement must be listed on the Requirements Register, and responsibility acknowledged in a Business Units Annual Compliance Plan.

For example; The Occupational Health and Safety Act is a Level 1 compliance requirement as the penalties and consequences of non-compliance can be severe. The Act is pervasive across all Business Units/Departments of the ELRC. The Act is a regulatory compliance.

4.4 Identifying and Managing Regulatory and Legislative Changes

Senior Managers are expected to identify changes to compliance requirements and obligations for which they are responsible, on a timely basis, and implement

the required changes to ensure that the ELRC continues to comply with its obligations.

There are a number of methodologies that can help business units meet the above expectations. Some of these include:

- Subscribe to legislative and regulatory updates provided by government, regulators and other sources;
- Subscribe to information services from external providers including regulators, legal firms, industry associations and professional research groups;
- Facilitate working groups with relevant business units and industry groups to interpret, coordinate and implement legislative change requirements;
- Build constructive and transparent relationships with the relevant regulatory and government bodies; and
- Manually monitor key information sources such as government, regulators and legal websites.

Senior Managers are responsible for discussing potential significant changes, such as the introduction of new regulation or legislation, with the General Secretary and the Internal Auditor. Significant changes could impact on the processes of more than one business unit and as such are likely require communication to many departments. The General Secretary will work with the Business Unit Senior Manager and other impacted business units to evaluate the impact of the change.

5. COMPLIANCE RISK ASSESSMENT

Risk is "**The chance of something happening that will have an impact on objectives."**

In the case of a compliance risk, the objective is adhering to compliance obligations, and thus compliance risk is; "the likelihood of something happening that could prevent the ELRC from complying with its obligations".

On at least an annual basis each Senior Manager must complete a risk assessment for the compliance requirements that fall within their area of responsibility, to identify the sources of compliance risk and ensure these risks are managed effectively and resources in managing compliance are prioritised efficiently.

5.1 Compliance Risk Management Process

Compliance Risk Management will be performed as follows:

5.1.1 Compliance risk assessments

Compliance risk assessments can be focused on categories of compliance obligations or requirements listed in the Compliance Risk Universe, however the risk universe is a tool for guidance only so risk assessments can be performed on other compliance areas if appropriate.

For example: Human Resources might perform compliance risk assessments focussing on the following areas, based on the risk universe:

Conditions of Employment, Salary Advice
Labour, Employee compensation
Employment Equity, Ethics

For guidance on performing a risk assessment, please refer to the ELRC Risk Management Framework.

In summary, the major steps of this process are as follows:

- Identify Risks;
- Identifying where the ELRC is at risk of non-compliance and what would be potential causes of non-compliance;
- Analyse the Risks (assess likelihood and impact);
- Determine how likely it is that non-compliance will occur and what is the consequence if it does;
- Evaluate the Risk;
- Determine the level and type of treatment required to mitigate the risk and develop a risk management plan.

Risk Management plans consist of a series of controls that will either reduce the likelihood of a risk occurring or reduce the consequence or impact if it does occur. The plans should be developed and implemented for all risks rated ‘Medium’ or above, where controls are not fully operational, in line with the Risk Management Framework.

The compliance risk assessment should be performed using the processes, systems and tools outlined in the ELRC’s Risk Management Framework.

5.1.2 Risk reporting and assurance requirements

The process for assessment and management of compliance risks should be in line with the Risk Management Framework and hence the reporting and assurance requirements for compliance risks follow that of any other risk.

In addition, any Medium or higher compliance risks for any priority Level 1 or 2 rated requirements, should be included on the Annual Compliance Plan for that Business Unit.

Accountabilities:

Ref.	Accountabilities
Divisional or Business Unit Manager	
(a)	Performing an annual assessment over the risk of non-compliance in their areas of responsibility. Documenting those risks and managing and reporting them in accordance with the Risk Management Framework
Internal Auditor	
(b)	Providing the risk management framework, tools, systems and support to enable ELRC to manage its compliance risks effectively.

6. MANAGE OBLIGATIONS

6.1 Ongoing Management

Managing compliance extends further than reporting compliance to legislators and regulators; it is about educating and raising awareness, ensuring our processes facilitate compliance, ensuring accountability for compliance and providing a mechanism for reporting and handling breaches and incidents.

6.2 Annual Compliance Plan (Attachment D)

Business units/Departments are required to complete an Annual Compliance Plan (see Attachment D) to document their compliance responsibilities, reporting, assurance and training requirements, and details of compliance risks rated ‘Medium’ or above, for the compliance obligations impacting on the operations of that business unit.

Sign-off of this plan is acknowledgement that the Business Unit/Departments recognises the compliance requirements and obligations affecting the processes of their business unit, that they will effectively manage the risks around meeting those requirements or obligations, and that they will complete any reporting, assurance or training responsibilities associated with those compliance requirements or obligations.

6.3 Reporting Potential Breaches of Compliance Requirements

A breach is defined as “an act or omission whereby ELRC has not met its compliance obligations, processes or behavioural obligations”.

Business Units are at the forefront of compliance management and are likely to be the origination of the reporting of potential breaches. Potential breaches can be identified from a number of sources, these include:

- Fines, penalties, damages or legal costs;
- Local, State, national or international adverse or unwanted publicity or media attention;
- Inquiry from the employer and related parties;
- Allegations of wrong doing, complaints from stakeholders or Whistleblowing reports;
- Death, injury or disability;
- OH&S incidents (it should be noted that the incident itself is not a breach and incidents can occur that are not associated with a compliance breach);
- Loss of staff morale;
- Criminal prosecution of ELRC, Executive or individual staff;
- Public allegations and/or civil claims relating to our corporate/business character, image or reputation;
- Outcomes from audit and assurance processes;
- Systemic errors / problems, loss of a customer or critical internal service;
- Detailed breach indicators and breach reporting criteria are contained in Attachment G.

All confirmed breaches must be recorded on the Breach Register in Attachment F.

6.4 Managing Potential Breach and Breach Outcomes

Following the reporting of a breach or a potential breach, the manager responsible should use the incident as an opportunity to identify the potential weakness in current processes that enabled the incident to occur in the first place, and also those areas in which to make process improvements.

Process improvements required resulting from a breach should be recorded in the Breach Reporting Form (**Attachment E**).

6.5 Records Management

Accurate up-to-date records of our compliance activities will be maintained to assist in the monitoring and review process and demonstrate conformity with the Compliance Management Policy. Records must be stored and managed in accordance with ELRC Records Management Policy.

7. MONITORING AND EVALUATION

For compliance management to be effective, performance of the compliance management processes should be continually monitored and measured. This includes the performance of individuals and business units in managing their own compliance obligations, but also the effectiveness, adequacy and appropriateness of the mechanisms used to manage compliance, i.e. the performance of the compliance management policy itself needs to be measured.

Performance can be measured through monitoring of achievement against defined key performance indicators or through internal or external assurance activities such as audits or reviews.

7.1 Performance Measures and Metrics

7.1.1 Individual and business unit performance

Individual and Business Unit/Department performance is to be reported through the quarterly management reporting processes, by means of measuring performance against predefined Key Performance Indicators (KPIs).

7.1.2 Compliance management policy performance

To ensure the compliance management policy is operating effectively at managing the obligations of the ELRC, its performance will be measured through internal audit review, which will assess its effectiveness, and appropriateness in managing compliance.

7.1.3 Performance indicators

Examples of KPIs which can be used are as follows:

Example KPIs	Rationale
Individual/ Business Unit	
Number of confirmed breaches	If Business Units/Departments are actively managing compliance the number of breaches should decrease.
Development and completion of annual compliance plans	By developing and completing compliance plans, Business Units/Departments are demonstrating their commitment to managing compliance.
Number of training sessions held Staff attendance at mandatory training sessions	If staff are educated and have knowledge of their compliance responsibilities, compliance obligations will be more actively managed.
Number of management plans in place for compliance risks	By developing risk management plans, the likelihood of compliance failures occurring should be reduced.
Number of compliance requirements of the business unit mapped to the Policy	The greater the number of compliance requirements mapped to the policy, the greater the assurance that compliance is being managed effectively.

Example KPIs	Rationale
Number of internal or external assurance Findings	If compliance is being managed effectively and improvements continually made, the number of assurance findings should decrease.
Timeliness in remedying compliance breaches or assurance findings	Findings and process improvements should be made on a timely basis to effectively manage compliance.
Compliance Management Policy	
Number of breaches and potential breaches reported from high priority compliance requirements	A successful policy will result in increased reporting and transparency.
Amount paid as a result of compliance breaches exceeding a particular threshold	A successful policy will reduce the amount paid in fines.
Number of confirmed breaches	A successful policy will reduce the amount of confirmed breaches.
Decrease in the rating of compliance Risks	A successful policy will improve the control structure and hence reduce the risk of compliance failure.
Alignment with King III on Compliance Management or other best practices in compliance management	The policy should remain up to date with best practices in order to manage compliance effectively.

7.2 Linkage to Assurance Activities

7.2.1 Compliance risks

Senior Managers must do an annual self-assessment on the operating effectiveness of the internal controls managing all 'Medium' to 'High' risks in their business unit/department or area of responsibility.

Controls and mitigation strategies for compliance risks will be subject to internal audit review as per the Risk Management Framework.

7.2.2 External assurance activities

Certain compliance requirements will require that audit or external reviews are carried out on a periodic basis. Where this is the case the Senior Manager of the business unit with primary responsibility for that compliance requirement is responsible for ensuring that this takes place.

Audit findings and recommendations

- The results of all assurance activities must be reported to the General Secretary and to the Audit Committee if required.
- In respect of any agreed findings or recommendations from assurance activities, Senior Managers with responsibility for the associated obligations or processes impacted are responsible for ensuring that the finding is remedied by the agreed due date.
- Where the results of the assurance activity have been reported to the Audit Committee, progress in remedying assurance findings will be reported to the Committee on a quarterly basis.
- The results of all assurance activities should be used as part of the continuous improvement process for compliance management and be

used as a mechanism to ensure that the organisation's processes are constantly progressed towards best practice.

7.2.3 Internal audit or other assurance activities

From time to time compliance with certain requirements and obligations will be subject to Internal Audit or other assurance reviews to provide assurance internally that obligations are being managed effectively and to ensure compliance processes are continuously improved.

Senior Managers are responsible for ensuring that internal audit staff have unrestricted access to all employees, records and property of the ELRC and are entitled to such information and explanations as they may require for audit purposes.

The responsibilities for reporting on audit findings and recommendations follows that detailed in 7.2.2 above.

7.2.4 Compliance management policy

Like other business processes, the Compliance Management Policy's design and implementation will be subject to independent review so that the following can occur:

- Gaps in the compliance universe can be identified and improved;
- Education needs throughout the ELRC can be identified and actioned;
- Potential and actual breaches can be understood, monitored, and reported; and any other deficiencies or inefficiencies can be understood and resolved.

The Compliance Management policy itself is therefore subject to review, including any component of the policy, such as the Obligations Registers, Annual Compliance Plans, Risk Registers, Breach Register, and other related inputs and sources of information as required.

Reviews may be undertaken as part of:

- Management self-assessments
- Internal Audits
- External Audit

The results of these audits will feed into our continuous improvement processes for managing compliance, including the compliance control environment.

7.3 Continuous Improvement

Continuous improvement provides a mechanism to maintain a relevant and effective Compliance Management policy. In this way continuous improvement serves to link potential or actual compliance failure with preventative of corrective action.

Compliance Management processes can continuously be improved through the following mechanisms:

- Implementing recommendations/findings from internal or external assurance processes;
- Reviewing compliance incidents, potential breaches or breaches to identify the causes.

Management is responsible for ensuring that they implement any agreed recommendations from internal or external assurance processes by the agreed deadlines, and are also responsible for ensuring that process improvements identified as a result of any breaches or potential breaches are implemented.

8. COMMUNICATION AND REPORTING

8.1 Communication

Managing compliance effectively requires continuous communication between internal and external stakeholders, and particularly with employees who are responsible for processes subject to compliance obligations, and also regular reporting on the results of compliance management practices.

Communication is required to:

- Raise awareness and understanding;
- Provide instruction;
- Monitor performance;
- Report performance; and
- Report breaches and incidents.

Internal stakeholders include employees (both permanent and casual), Executives, and Committees.

External stakeholders could include relevant government bodies and organisations, outsource providers, contractors, suppliers, customers or regulatory bodies.

Senior Managers should consider the type of compliance requirements and obligations for which they are responsible, and if a significant amount of communication to stakeholders is required to manage obligations effectively, a

communication plan should be developed to help ensure that the appropriate information is communicated on a timely basis in the appropriate manner to the appropriate stakeholders.

Communication Plans

A communication plan would typically include:

- Description of the compliance obligation
- A description of the information to be communicated
- The purpose of the communication
- Identification of audience: who they are and whether they are internal or external stakeholders
- Type of communication method. Communication methods include:

    - Compliance training
    - The intranet
    - Management meetings
    - Posting items on the wall in highly frequented areas
    - Reporting processes
    - Leading by example
    - Mentoring; and
    - Questionnaires

- Frequency or timing of communication
- Expected response or level of stakeholder involvement (if applicable)

8.2 Training and Education

All staff have compliance obligations and should be competent to discharge these effectively. Competence can be attained through education, training or work experience.

Management is responsible for ensuring that staff have the required level of competency to meet their compliance obligations, they are therefore required to make sure that compliance requirements are addressed in the ELRC's training programs and that their staff attend the appropriate sessions.

8.3 Reporting

The format, content and timing of internal compliance reporting, unless prescribed by law, is tailored to the nature of the issue being reported as per the following guidelines:

- Incidents and potential breaches are reported as and when they occur, to business unit management;
- Reporting on performance for Compliance risks is as per the Risk Management Policy;
- Results of assurance activities are reported to the General Secretary and the Audit Committee as required; and
- During the year, compliance issues will be reported as required on a quarterly basis in the Audit Committee Meetings.

8.4 Breach Management and Reporting

Compliance breaches must be reported and managed in accordance with the Breach Reporting Process and assessed utilising the Breach Assessment Criteria.

Policy requirements for this are as follows:

Breach Management Requirement	**Accountability**
Notify Management or Internal Auditor	Staff member identifying incident
Assess the significance of the breach using Breach Assessment Criteria	Internal Auditor
Report confirmed breaches in line with policy	Internal Auditor

Breach Reporting:

	Breaching Rating		
Reporting Requirements	High	Medium	Low
Audit Committee	❑ ❑ ❑	❑ ❑	❑
General Secretary	❑ ❑ ❑	❑ ❑	❑
Senior Management and Internal Auditor	❑ ❑ ❑	❑ ❑	❑

ATTACHMENT A: Compliance Register

Name: Labour Relations Act**, No. 66 of 1995**
Category: Core
Inherent Indicator: High

NO.	SECTION	DESCRIPTION	REQUIREMENT	YES	NO	N/A	COMMENTS
1.	28	Powers and functions of bargaining Council	Does the powers and functions of the ELRC in relation to its registered scope include the following: (a) To conclude collective agreements? (b) To enforce those collective agreements? (c) To prevent and resolve labour disputes? (d) To perform the dispute resolution functions referred to in section 51? (e) To establish and administer a fund to be used for resolving disputes? (f) To promote and establish training and education schemes?	**Yes**			

Act Name: Occupational Health & Safety Act 85 of 1993
Category: Secondary
Inherent Indicator: Medium

NO.	SECTION	DESCRIPTION	REQUIREMENT	YES	NO	N/A	COMMENTS
1.	7	Health and Safety policy	Does a written policy concerning the protection of the health and safety of the employees at work exist?				

Act Name: Employment Equity Act 55 of 1998
Category: Secondary
Inherent Indicator: Medium

NO.	SECTION	DESCRIPTION	REQUIREMENT	YES	NO	N/A	COMMENTS
1.	5	Elimination of unfair discrimination	An employer must take steps to promote equal opportunity in the workplace by eliminating unfair discrimination in any employment policy or practice.				

ATTACHMENT B: Obligations Register (Compliance Requirement)

Compliance Requirement	Requirement name	**Priority Rating**	Level 1, 2 or 3	**Administrative Body**	Name of Administrative Body
Type of Requirement		**Primary Responsibility**	Business Unit Name Manager Name		

Reporting Obligations

Ref	Obligation	Due Date	Manager Responsible

Audit/assurance Obligations

Ref	Obligation	Due Date	Manager Responsible

Other Obligations

Ref	Obligation	Responsibility for Management	Business Areas or processes affected	Related Internal Policy or Procedure Document	Obligation included in policy?	Process meeting obligation

ATTACHMENT C: Responsibility Map (Compliance Requirement)

The responsibility map documents the coverage of a particular compliance requirement in relation to the entire organisation and includes a description of the requirement and its obligations. The responsibility map is used by the business unit with primary responsibility for managing the compliance requirement to communicate this coverage within the business unit and to other stakeholders as required.

Compliance Requirement:

For example: Labour Relations Act, No. 66 of 1995

Scope:

Include a brief description of the purpose of the requirement and its coverage in relation to the ELRC.

Primary Responsibility:

Identify the business unit with primary responsibility.

Business Unit	Nature of Responsibility	Manager Responsible

Secondary Responsibilities:

Identify the business units that have responsibilities to manage obligations under this compliance requirement and the obligations they manage. The business unit with primary responsibility is not expected to manage these obligations but monitors that the business unit with secondary responsibility knows which obligations they are responsible for.

Business Unit	Nature of Responsibility	Manager Responsible

Tertiary Responsibilities:

Some compliance requirements may require awareness and understanding by a wider group outside those business units who have Primary or Secondary responsibilities for managing obligations.

ATTACHMENT D: Annual Compliance Plan Template

This template, except for the sign-off, will be completed by business unit Managers at the start of each financial year to help document all relevant elements of their compliance program. At the end of each year as part of the annual reporting process, business unit managers will be asked to "certify" that they have complied with their plan.

1. Primary Compliance Responsibilities

Record the requirements where this business unit has overall responsibility for management of the ELRC. This table will be populated with information from the **Compliance Register**.

Requirement	Type of requirement	Priority Rating	Manager Responsible

2. Secondary Compliance

Record responsibilities where primary responsibility lies with another business unit, but this business unit is responsible for compliance with certain obligations. Information for this table will come from the **Compliance Register.**

Requirement	Type of requirement	Priority Rating	Primary Owner	Secondary Manager Responsible

3. Audit and Assurance Requirements

Record audit and assurance activities, both internal and external, planned to monitor compliance activities in the business unit.

Requirement	Nature of Audit/Assurance	Due date

4. Training Requirements

Record compliance training sessions, internal and external, to be undertaken by business unit management and staff during the year.

Requirement	Nature of Training	Due date

Sign-off
Sign off is to be completed at the start and end of each year. Signed forms are to be sent to the Internal Auditor.

Start of Year - I agree that these are the compliance requirements relating to my business unit and operations and that I will manage them and will report all potential breaches in accordance with the breach reporting process.

Signature: _____

Print Name: _____

Title: _____

Date: _____

End of Year - I confirm that all the compliance requirements and obligations of this Business Unit were managed in accordance with the Compliance Management policy, all breaches and potential breaches have been reported in line with the breach reporting process, and all training, assurance and reporting requirements have been completed.

Signature: _____

Print Name: _____

Title: _____

Date: _____

ATTACHMENT E: Potential Breach Reporting Form

Business Unit:		**Breach Report Completed By:**	
Identified by:		**Date identified:**	

Summary of Potential Compliance Breach:	
Type of Potential Compliance Breach: (tick appropriate)	
Legislation:	
Internal Policy and Procedure:	
Assessment of Potential Breach (High, Medium, Low)	
Justification of Assessment (describe the rationale behind the assessment rating)	
Assessment signed-off by Internal Auditor	

ATTACHMENT F: Breach Register Template

The Compliance Manager will own the breach register and will use the potential breach register template to source information about the breach. This register is to be used only for confirmed breaches.

Date Breach Discovered	Date(s) of Breach	Description of Breach	Person Responsible	How was breach identified?	Process & Responsibilities for Handling Breach	Date Breach Rectified and Closed

ATTACHMENT G: Criteria or Indicators of Compliance Breaches (In Line With Risk Analysis Criteria)

Note: The criteria are below for guidance in determining the appropriate level of breach escalation only as the nature of every potential breach will vary. Each potential breach or indicator should be assessed on a case-by-case basis and reported as considered appropriate by the responsible Manager. If assistance is required, please contact the Internal Auditor.

Note: The criteria are below for guidance in determining the appropriate level of breach escalation only as the nature of every potential breach will vary. Each potential breach or indicator should be assessed on a case-by-case basis and reported as considered appropriate by the responsible Manager. If assistance is required, please contact the Internal Auditor.

	Potential Significant Breach		Potential Insignificant Breach
Indicators	High	**Medium**	**Low**
Financial			
Costs – includes damages, fines, penalties, legal costs, loss of management time			
Reputation/Political			
Local, State, National adverse or unwanted publicity or media attention			
Allegations of wrong doing, complaints from stakeholders or whistleblowing reports			
People & Safety			
Death, injury or disability			
Industrial action or union activity			
Loss of staff moral			
Legal & Compliance			
Criminal prosecution of ELRC, Executive or individual staff; or result in potential liability of an Executive			
Customer Service Interruption			
Systemic errors / problems, loss of customer service			
Operational Effectiveness			

	Potential Significant Breach		Potential Insignificant Breach
Indicators	High	**Medium**	**Low**
Systemic errors / problems, loss of an internal service or management time			