KOUGA
local municipality
Good Governance through Service Excellence

ICT Risk Management Framework

DOCUMENT INFORMATION SHEET

Title of Report	:	*ICT Risk Management Framework*
Type of Report	:	*Policy*
Document Number	:	
Prepared By	:	Allister Makomo
Typed By	:	Allister Makomo
Reviewed By	:	*KPMG Services (Pty) Ltd*
Functional Area	:	*Financial Services - IT*
Prepared For	:	*Kouga Local Municipality*
Date of Issue	:	*15 November 2016*

Kouga Municipality
Approved: 29 March 2018 Item: 18/03/F1

DOCUMENT CONTROL SHEET

The purpose of this form is to ensure that documents approved prior to issue. The form is to be bound into the front of all documents released by Kouga Local Municipality.

Title of Report	:	*ICT Risk Management Framework*
Type of Report	:	*Policy*
Document Number	:	

SIGNING OF THE ORIGINAL DOCUMENT

This framework is approved by the signatories listed below whom by signing this document confirm their acceptance of its content and authorise the implementation/adoption thereof.

Signature: ICT Manager — Date: 15/05/2018

Signature: Chief Financial Officer — Date: 15/5/2018

Signature: Municipal Manager — Date: 15/5/2018

Signature: Mayor — Date

29 March 2018
Council Date of Approval

REVISION CONTROL CHART

The purpose of this form is to ensure that documents are reviewed. The form is to be bound into the front of all documents released by Kouga Local Municipality.

REVISION 1	Prepared By:	Reviewed By:	Approved By:
Date:	Signature:	Signature:	Signature:
Description of changes:			

REVISION 2	Prepared By:	Reviewed By:	Approved By:
Date:	Signature:	Signature:	Signature:
Description of changes:			

REVISION 3	Prepared By:	Reviewed By:	Approved By:
Date:	Signature:	Signature:	Signature:
Description of changes:			

TABLE OF CONTENTS

DOCUMENT ADMINISTRATION

Glossary of Terms

Term	Description
Risk Management	The process of planning, organizing, staffing, leading, and controlling an organization's resources to minimize the possibility of loss or non-achievement of objectives caused by risk.
Risk Appetite	The extent of willingness to take risks in the pursuit of the business objectives.
ERM	Enterprise Risk Management
CGICTPF	Corporate Governance of ICT Policy Framework
Corporate Governance	"…The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly." – IT Governance Institute "Procedures and processes according to which an organisation is directed and controlled." – Organisation of Economic and Co-operation Development
Corporate Governance of ICT	"The system by which the current and future use of ICT is directed and controlled." – ISO/IEC 38500 "Corporate governance of ICT involves evaluation and directing the use of ICT to support the organisation, and monitoring this use to achieve plan. It includes the strategy and policies for using ICT within an organisation." – ISO/IEC 38500
DPSA	Department of Public Service and Administration
Executive Management	The Executive Management of the Municipality is made up of the Head of Department and all Chief Directors of the Department. This normally constitutes the Executive Committee of the Municipality and should include the GITO.
GICT	Corporate Governance of ICT
ICT	Information and Communications Technology, also referred to as **IT**
Governance Champion	The Manager in the municipality who is responsible to drive Corporate Governance of and Governance of ICT.
Governance of	"The effective and efficient management of IT resources to facilitate the

ICT	achievement of company strategic objectives." – King III Code, 2009 "Is the responsibility of executives and the municipal council, and consists of the leadership, organisational structures and processes that ensure that the municipality's IT sustains and extends the municipal strategy and objectives." – ITGI, 2005
Governance Principles	"The vehicle to translate the desired behaviour into practical guidance for day-to-day management." – COBIT 5 Framework, 2012
ISO/IEC 38500	International Standard on Corporate Governance of ICT
IT	Information Technology, also referred to as ICT
MISS	Minimum Information Security Standards
MIOS	Minimum Interoperability Standards
RACI	Responsibility, Accountability, Consulting, Information
AGSA	Auditor General of South Africa

ICT RISK MANAGEMENT FRAMEWORK

1. Introduction

Section 195 of the Constitution of the Republic of South Africa emphasizes the values and principles underlining public administration, which include the efficient, economic, and effective use of resources in the public sector. It also provides for a public administration that is accountable and transparent through the provision of timely, accessible and accurate information.

In addition to the constitutional provisions, the public service regulations provide for the implementation of a management framework for the entire public service. Planning is very important in clarifying the intentions of an organisation, facilitating the allocation of budgets according to priorities; monitoring results and enforcing accountability in the department.

Embedded within this planning framework is an internal control and risk management framework that serves to ensure that the ICT department achieves its outcomes and risk management is undoubtedly one of the most important management tools.

1.1. Purpose and Applicability

This ICT Risk Management Framework ensures that key risks are identified, measured and managed. This framework provides management with proven risk management tools that support their decision-making responsibilities and processes, while managing risks which impact on the attainment of the municipality's strategic objectives (as outlined in the municipal IDP).

Risk Management is everyone's responsibility and therefore it must be embedded into the everyday activities of the municipality. This implies that ICT Risk Management must be part of every decision that is made, every objective that is set and every process that is designed throughout the municipality.

The purpose of this ICT Risk Management Framework is to:

- Advance the development and implementation of modern management practices and to support innovation throughout Kouga Local Municipality;
- Contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the municipal and citizens interest, maintain municipal trust, and ensure due diligence;
- Provide a comprehensive approach to better integrate risk management into strategic decision making;
- Set the context in which risks are managed, in terms of how they will be identified, analyzed, controlled, monitored, and reviewed;
- Ensure that information security requirements, including necessary security controls, are integrated into municipality's ICT environment and system development life cycle processes.

2. Context Establishment

The external and internal context for ICT risk management are established within the municipality, which involves setting the basic criteria necessary for ICT risk management, defining the scope and boundaries, and establishing an appropriate organization operating ICT risk management. It is essential to determine the purpose of ICT risk management as this affects the overall process and the context establishment in particular. For Kouga Local Municipality, this purpose is:

- Supporting an Information Security Management System (ISMS)
- Legal compliance and evidence of due diligence
- Preparation of a business continuity plan
- Preparation of an incident response plan

— Description of the information security requirements for municipal services

2.1. General Considerations and Criteria

Depending on the scope and objectives of the risk management exercise, different approaches can be applied. The approach might also be different for each iteration. An appropriate risk management approach should be selected or developed that addresses basic criteria such as: risk evaluation criteria, impact criteria, risk acceptance criteria. Additionally, municipal management should assess whether necessary resources are available to:

— Perform risk assessment and establish a risk treatment plan

— Define and implement policies and procedures, including implementation of the controls selected

— Monitor controls

— Monitor the ICT risk management process

As a result, risk evaluation criteria should be developed by management for evaluating ICT risk considering the followings:

— The strategic value of the business information process

— The criticality of the information assets involved

— Legal and regulatory requirements, and contractual obligations

— Operational and business importance of availability, confidentiality and integrity

— Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation

Further, impact criteria should be developed and specified in terms of the degree of damage or costs to the municipality caused by an information security event considering the following:

- Level of classification of the impacted information asset
- Breaches of information security (e.g. loss of confidentiality, integrity and availability)
- Impaired operations (internal or third parties)
- Loss of business and financial value
- Disruption of plans and deadlines
- Damage of reputation
- Breaches of legal, regulatory or contractual requirements

Furthermore, risk acceptance criteria should be developed and specified by municipal management. Risk acceptance criteria should depend on the municipality's policies, goals, objectives and the interests of stakeholders. As such, the municipality should define its own scales for levels of risk acceptance. The following should be considered during development:

- Risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances
- Risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk
- Different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in noncompliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement

— Risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period

Risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity. Risk acceptance criteria should be set up considering the following:

— Business criteria

— Legal and regulatory aspects

— Operations

— Technology

— Finance

— Social and humanitarian factors

2.2. Scope and Boundaries

Municipal management should define the scope and boundaries of ICT risk management. The scope of the ICT risk management process needs to be defined to ensure that all relevant assets are taken into account in the risk assessment. In addition, the boundaries need to be identified to address those risks that might arise through these boundaries.

Information about Kouga Local Municipality should be collected to determine the environment it operates in and its relevance to the ICT risk management process.

When defining the scope and boundaries, management should consider the following information:

— The municipality's strategic objectives, strategies and policies

— Municipal processes

- The municipality's functions and structure
- Legal, regulatory and contractual requirements applicable to the municipality
- The municipality's information security policy
- The municipality's overall approach to risk management
- Information assets
- Locations of the municipal premises and their geographical characteristics
- Constraints affecting the municipality
- Expectation of stakeholders
- Socio-cultural environment
- Interfaces (i.e. information exchange with the environment)

Additionally, management should provide justification for any exclusion from the scope. Examples of the risk management scope may be an ICT application, ICT infrastructure, a municipal process, or a defined part of the municipality.

2.3. Roles and Responsibilities

- All employees of the municipality are affected and have some responsibility in assisting ICT in implementing ICT risk management;
- The ICT Manager is ultimately responsible for ICT risk management and assumes overall ownership. Further, The ICT Manager is responsible for updating and maintaining the ICT risk register
- Other directorates support the ICT risk management philosophy, promote compliance with the risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances

— The ICT Steering Committee will ensure review and approval of all ICT risk management endeavours

— The Audit and Risk Committee will provide ICT risk management oversight

— A number of external stakeholders often provide information useful in effecting risk management, but they are not responsible for the effectiveness of the municipality's risk management.

3. Risk Assessment

Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment.

Risk assessment is often conducted in two (or more) iterations. First, a high level assessment is carried out to identify potentially high risks that warrant further assessment. The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration. Where this provides insufficient information to assess the risk then further detailed analyses are conducted, likely on parts of the total scope, and possibly using a different method.

It is up to the municipal management to select its own approach to risk assessment based on the objectives and the aim of the risk assessment.

3.3. Risk Identification

During the phase of risk identification, management considers external and internal, as well as financial and non-financial factors that influence the municipality's policy and management agenda.

Identifying major trends and their variation over time is particularly relevant in providing early warnings.

Some external factors to be considered for potential risks include:

— Political: the influence of international governments and other governing bodies;

— Economic: international, national markets and globalizations;

— Social: major demographic and social trends, level of citizen engagement; and

— Technological.

Internal factors reflect management's choices and include such matters as:

— The overall management framework;

— Governance and accountability frameworks;

— Level of transparency required;

— Values and ethics;

— Infrastructure;

— Policies, procedures and processes;

— Human resource capacity; and

— Technology.

Within Kouga Local Municipality, ICT related risks are categorized in the following focus areas:

— **Business focus**: This is the risk that the strategic requirements and user needs are not met by ICT or ICT is not appropriately aligned to the municipality's IDP strategy and future plans.

— **Information assets**: This is the risk that the very nature of the data and information ("information assets") held by the municipality could result in a loss.

- **Dependence on ICT**: This risk describes the impact of the loss of parts of the ICT-infrastructure. The more dependent the municipality is on their ICT systems, the higher is the potential loss, whether direct financial loss or reputational loss.
- **Dependence on ICT Internal staff**: This is the risk that the nature and extent of the municipality's dependence on its own ICT staff could lead to a loss being suffered.
- **Dependence on Third Parties**: This is the risk that the municipality could suffer a loss as a result of its dependence on third parties such as outsourcers/co-sourcers, suppliers, contractors and consultants.
- **Reliability of ICT Systems**: This is the risk that a lack of reliability in the ICT systems could lead to a loss being suffered by the municipality.
- **Changes to ICT**: This describes the risk of losses as a result of the degree of changes to the ICT environment.
- **Legislative and Regulatory Environment**: This is the risk that lack of compliance with legislation relating to the processing, storage and use of information might lead to a financial or reputational loss to the municipality.

3.4. Risk Analysis

Risk analysis allows the ICT department to consider how potential events might affect the achievement of objectives. Management assesses risk events by analyzing their impact and likelihood using the scales below.

Impact Parameters

Severity Ranking	Continuity of Service Delivery	Safety & Environmental	Technical Complexity	Financial
Critical 5	Risk event will result in widespread and lengthy reduction in continuity of service delivery to the general public for a period greater than 48 hours	Major environmental damage. Serious injury (permanent disability) or death of personnel or members of the public. Major negative media coverage.	Use of unproven technology for critical systems / project components. High level of technical interdependencies between system components.	Can lead to termination of municipal activity
Major 4	Reduction in service delivery or disruption for a period ranging between 24 & 48 hours over a significant area	Significant injury of personnel or public. Significant environmental damage. Significant negative media coverage.	Use of new technology not previously utilized by the municipality for critical systems / project components.	Cost increase > 10%
Moderate 3	Reduction in service delivery or disruption for a period between 8 & 24 hours over a significant area	Lower level of environmental, safety or health impacts. Negative media coverage	Use of unproven or emerging technology for critical systems / project components.	Cost increase > 5%
Minor 2	Brief local inconvenience (work around possible). Loss of an asset with minor impact on operations	Little environmental, safety or health impacts. Limited negative media coverage.	Use of unproven or emerging technology for systems / project components.	Cost increase < 1%
Insignificant 1	No or minimal impact on municipal services or core systems	No environmental, safety or health impacts and/or negative media coverage	Use of unproven or emerging technology for non-critical systems / project components	Minimal or no impact on cost

Likelihood Parameters

Probability Factor	Measurement Criteria	Qualification Criteria	Rating
Common	The risk is already occurring, or has a high likelihood of occurring more than once during the next 12 months	The risk is almost certain to occur in the current circumstances	5
Likely	The risk will easily occur, and is likely to occur at least once during the next 12 months	More than an even chance of occurring	4
Moderate	There is an above average chance of the risk occurring more than once during the next 3 years	Could occur often	3
Unlikely	The risk has a low likelihood of occurring during the next 3 years	Low likelihood, but could happen	2
Rare	The risk is unlikely to occur during the next 3 years	Not expected to happen - event would be a surprise	1

Inherent risk rating = impact X likelihood

Residual Risk

Residual risk is determined by taking into account the adequacy of the risk mitigating controls in place.

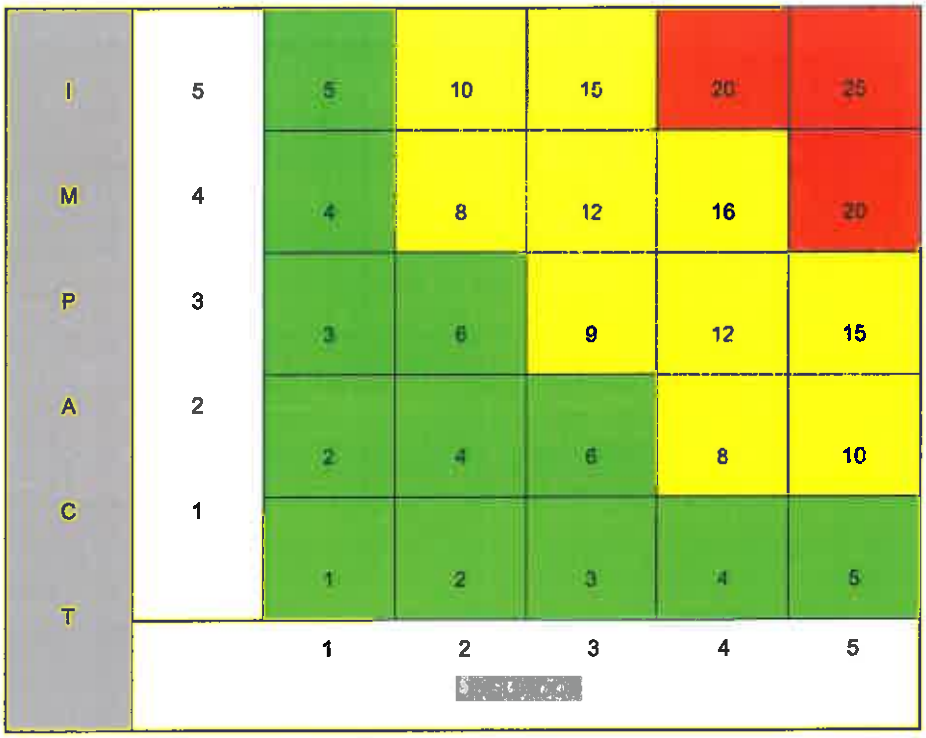
Control adequacy scales:

Adequacy Factor	Adequacy Qualification Criteria
Over-controlled 90%	The risk is adequately controlled and managed, but in some regards over-controlled.
Adequate 80%	The majority of risk exposure is adequately controlled and managed.
Partially adequate 50%	Some of the risk exposure appears to be adequately controlled, but there are major deficiencies.

Inadequate 20%	Control measures are mostly inadequate.

Residual risk = Inherent risk – control adequacy

The high, medium and low risk parameters can be depicted using the following risk matrix:



In order to assist in determining risk acceptability, the following thresholds should be used as guidelines;

Thresholds Where the result is:	Threshold Interpretation	Suggested Action	Suggested Timing
Between 17 and 25	**RED – Unacceptable** High Risk	Management should take immediate action to reduce risk exposure to	Immediate action required

			an acceptable level.	
Between 8 and 16		**YELLOW – Cautionary** Medium Risk	Management should constantly monitor the risk exposure and related control adequacy.	Medium term action - within three months
Between 1 and 7		**GREEN – Acceptable** Low Risk	Management should monitor risks and may consider reducing the cost of control.	Monitor – no immediate action required

Likelihood represents the possibility that a given event will occur, while impact represents its effect should it occur. Estimates of risk likelihood and impact will be determined using data from past observable events, which may provide a more objective basis than entirely subjective estimates.

Internally generated data based on the municipality's own experience will reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data are a primary input, external data will be useful as a checkpoint or to enhance our analysis.

3.5. Risk Evaluation

To evaluate risks, the municipality should compare the estimated risks with the risk evaluation criteria defined during the context establishment. Risk evaluation criteria used to make decisions should be consistent with the defined external and internal ICT risk management context and take into account the objectives of the municipality and stakeholder views etc. Decisions as taken in the risk evaluation activity are mainly based on the acceptable level of risk. However, consequences, likelihood, and the degree of confidence in the risk identification and analysis should be considered as well. During the risk evaluation stage, contractual, legal and regulatory requirements are factors that should be taken into account in addition to the estimated risks. Aggregation of multiple low or medium risks may result in much higher overall risks and need to be addressed accordingly.

Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future actions. Decisions should include:

— Whether an activity should be undertaken

— Priorities for risk treatment considering estimated levels of risks

As an output from this phase, there is a list of risks that is prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks in order to effectively and efficiently perform risk treatment.

4. Risk Treatment

Municipal management will identify risk response strategy options referred to as either risk treatment or risk responses, and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter design and implement response options.

The consideration of risk responses is essential to risk management and requires that management select a response that is expected to bring risk likelihood and impact within ICT's risk tolerance level.

After the risks have been identified and the contributing factors or root causes have been established, the control strategy will be identified for the various risk exposures. Risk responses will fall within the categories of risk avoidance, active management and acceptance. The following will be used to identify the control strategies considered by management:

— Risk Modification;

— Risk Retention;

— Risk Avoidance; or

— Risk Sharing.

4.1. Risk Modification

Appropriate and justified controls are selected to meet the requirements identified by the risk assessment and risk treatment. This selection takes account of the risk acceptance criteria as well as legal, regulatory and contractual requirements. This selection should also take account of cost and timeframe for implementation of controls, or technical, environmental and cultural aspects.

In general, controls may provide one or more of the following types of protection: correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring and awareness. During control selection it is important to weigh the cost of acquisition, implementation, administration, operation, monitoring, and maintenance of the controls against the value of the assets being protected. Furthermore, the return on investment in terms of risk reduction and potential to exploit new business opportunities afforded by certain controls should be considered. Additionally, consideration should be given to specialized skills that may be needed to define and implement new controls or modify existing ones.

There are many constraints that can affect the selection of controls. Technical constraints such as performance requirements, manageability (operational support requirements) and compatibility issues may hamper the use of certain controls or could induce human error either nullifying the control, giving a false sense of security or even increasing the risk beyond not having the control (e.g. requiring complex passwords without proper training, leading to users writing passwords down). Moreover, it could be the case that a control would affect performance. Municipal management should try to identify a solution that satisfies performance requirements while guaranteeing sufficient information security. The result of this step is a list of possible controls, with their cost, benefit, and priority of implementation.

Within Kouga Local Municipality, ICT-related controls for mitigating identified risks are grouped into the following categories and sub-categories:

— Management of ICT

- Council / Senior management involvement
- ICT strategy
- ICT cost and investment management
- Management reporting of ICT performance
- Service level management
- Legal and regulatory compliance
- Human Resource management
- End user computing
- Management of third party services

— Continuity of systems

- Backup of data and systems
- Capacity management
- Incident and problem management
- Continuity planning
- Operations management
- Configuration management

— Physical security and environmental controls

- Physical access control
- Protection of the environment

— Security of information and systems

- Security policy
- Security administration
- Logical access control facilities
- External communications

— System development and change management

- Development methodology
- Project management
- User participation
- Quality and project assurance
- Documentation
- Business change process
- Technical change management

— Control Assurance

- Audit of ICT
- Risk management
- Assessment of control adequacy

4.2. Risk Retention

If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.

4.3. Risk Avoidance

When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated. For example, for risks caused by nature it may be most cost effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control.

4.4. Risk Sharing

Risk sharing involves a decision to share certain risks with external parties. Risk sharing can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary.

Sharing can be done by insurance that will support the consequences, or by sub-contracting a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

It should be noted that it may be possible to share the responsibility to manage risk but it is not normally possible to share the liability of an impact. The general public (serving community) will usually attribute an adverse impact as being the fault of the municipality.

5. Risk Acceptance

Risk treatment plans should describe how assessed risks are to be treated to meet risk acceptance criteria. It is important for responsible municipal managers to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval.

In some cases, the level of residual risk may not meet risk acceptance criteria because the criteria being applied do not take into account prevailing circumstances. For example, it might be argued that it is necessary to accept risks because the benefits accompanying the risks are very attractive, or because the cost of risk modification is too high. Such circumstances indicate that risk acceptance criteria are inadequate and should be revised if

possible. However, it is not always possible to revise the risk acceptance criteria in a timely manner. In such cases, decision makers may have to accept risks that do not meet normal acceptance criteria. If this is necessary, the decision maker should explicitly comment on the risks and include a justification for the decision to override normal risk acceptance criteria.

Therefore, if this occurs, there should be a list of accepted risks with justification for those that do not meet the municipality's normal risk acceptance criteria formally documented and signed off by municipal management.

6. Risk Communication and Consultation

Pertinent information – both from internal and external sources, financial or non-financial – should be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication should also occur in a broader sense, flowing down, across and up the municipality, as well as the exchange of relevant information with external parties, such as the general public, suppliers, regulators and shareholders.

An array of information should be used, relevant to one or more objectives categories. Management should establish an information systems infrastructure to source, capture, process, analyze and report relevant information. These information systems – will usually be computerized but also involving manual inputs or interfaces – often will be viewed in the context of processing internally generated data relating to transactions. This will allow the municipality to track actual performance against targets, plans and expectations. It will also provide insights into how the municipality performed under varying conditions, allowing municipal management to identify correlations, trends and to forecast future performance. Historical data also would provide early warnings of potential events that warrant municipal management attention.

Present or current state data would allow the municipal ICT department to assess its risks at a specific point in time and remain within established risk tolerances. Current state data would allow management to take a real-time view of existing risks inherent in a process,

function or unit and to identify variations from expectations. This would provide a view of ICT's risk profile, enabling municipal management to alter activities as necessary to fit in with the acceptable level of risk

Municipal Management should keep the Audit and Risk Committee up-to-date on performance, developments, risks and the functioning of risk management, and other relevant events and issues. The more effective the communication, the more successful the Audit and Risk Committee will be in carrying out its oversight responsibilities, in acting as an executive authority on critical issues and in providing advice, counsel and direction.

The ICT Manager should keep track of all ICT related issues and risks by maintaining an ICT risk register, with major risks being consolidated into the overall municipal risk register and communicated to the Audit and Risk Committee. It will remain the responsibility of the ICT manager to periodically perform risk assessments on the ICT environment and controls, and to duly update the ICT risk register accordingly. Risk assessments shall be performed at least bi-annually, or as changes are introduced into the ICT environment.

7. Risk Monitoring and Review

Risk management should be regularly monitored – a process that assesses both the presence and functioning of components and the quality of their performance over time. Monitoring should be done in two ways: through ongoing activities or separate evaluations. This will ensure that risk management continues to be applied at all levels and across the municipality.

Ongoing monitoring should be built into the normal, recurring operating activities and should be performed on a real-time basis.

Key risk indicators

Key risk indicators will assist municipal management to monitor risks. Key risk indicators have two focal points i.e. the inherent risk itself as well as losses, incidents and variances. Each key risk will have a key risk indicator to serve as a risk warning mechanism.

Each section will be responsible for defining, monitoring and reporting on key risk indicators for all key risks identified.

Risk tolerance limits

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances should be measured in the same units as the related objectives.

Performance measures should be aligned to help ensure that actual results will be within the acceptable risk tolerances. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances will provide management with greater assurance that the department remains within its risk appetite and, in turn, provide a higher degree of comfort that the department will achieve its objectives. Each departmental section will be responsible for defining its own risk tolerance limits for all key risks identified.

8. Exceptions

Deviations from this framework and its associated policies/procedures will only be permitted in the following circumstances:

a) When specific provisions have been made for it in the ICT steering committee meetings or municipal management meetings (reasons for allowing non-compliance shall be documented within the minutes of meetings, and formal approval sought per written permission)

b) On written permissions of the municipal manager of Kouga Local Municipality (reasons for allowing non-compliance to one or more aspects of the policy shall be clearly stated in such permission; no blanket non-compliance shall be allowed under any circumstances)

9. Monitoring of Compliance

The municipal council, with the assistance of the ICT steering and audit committees, must ensure compliance with this framework and its associated policies/procedures.

The ICT manager shall frequently report on the compliance with this framework, and report such compliance to the ICT steering committee. In the event of non-compliance or insufficient progress, such findings shall be reported to the municipal manager.

Municipal management hereby reserves the right to action disciplinary reform on both the ICT steering committee and ICT manager should compliance to this policy not be satisfactory. Such reforms may take the form of verbal and written warnings, or at worst, termination of contract or employment.

10. Review and Update Process

The ICT manager, assisted by the ICT steering committee, must ensure that this policy and its associated policies/procedures are reviewed and updated after two years at most, or as and when necessary.

APPROVED BY COUNCIL ON : **29 MARCH 2018**

ITEM NO. : **18/03/F1**