DIGICALL

IT RISK MANAGEMENT POLICY V1.3

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.3
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		05.09.2024
Ameet Ranchod	IT Infrastructure Manager		30/09/2024
Johan Kriel	Group CIO		24/10/2024

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	25.02.2020	Ameet Ranchod	Document Creation
0.9	25.02.2020	Ameet Ranchod	Final Draft
1.0	25.02.2021	Ameet Ranchod	Version 1.0
1.1	31.05.2022	Celeste Ramnarayan	Version 1.1
1.2	01.07.2023	Donald Fraser	Updated personnel & roles
1.3	01.08.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

This policy applies to all employees and contractors during the performance of company related business and duties.

2 Policy Statement

In addition to this policy, the Digicall Group will conduct ongoing assessments of threats and risks related to information assets, to determine the necessity of safeguards, countermeasures, and controls.

In the Digicall Group Risk Management Policy the Digicall Group will be averse to IT risk.

The Digicall Group will continuously monitor for any change in the threat environment and make any adjustment necessary to maintain an acceptable level of risk. The Digicall Group risk management process will include:

1. Identifying key information assets and subjecting them to IT specific risk assessments.
2. Identifying level of compliance to Industry best practice for risk management and Information Security.
3. Assessing exposure to a list of common threats and vulnerabilities.
4. Maintaining risk registers, which include information security and operational risks.
5. Implementing technical, policy, Business Continuity, and management initiatives to reduce or eliminate identified risks.
6. Regular reviews of the performance and effectiveness of implemented controls.
7. Reporting significant risks to the Digicall Group Management Team.

The basic approach that has been adopted for assessing the risks is based on the following key activities:

1. Asset and Risk Identification.
2. Business Impact Assessment.
3. Risk Assessment.
4. Identifying the threats and vulnerabilities related to these assets.
5. Calculating the resulting risk exposure and impact.
6. Agreeing controls, activities, and processes to treat risks.
7. Implementing risk treatment initiatives and controls.

Regular reviews of the asset list and the business risk profile are part of the risk assessment approach for information security. This enables compliance with the policy to be checked as well as the ongoing effectiveness of the implemented controls.

3 Purpose

The purpose of risk assessment is to identify security threats and evaluate any associated risks to business arising from Digicall Group activities, enabling informed decisions to be taken to eliminate or minimize any risk to business. In many cases a risk assessment will lead to the clarification and

documenting of local team protocols and procedures that are often already in place. The analytical process involved with risk assessment and control can also result in efficiencies in existing processes being identified. Risk assessments can also assist in the identification of requirements for, and levels of, instruction, information, training, and supervision that may be required for the activity.

4 General

4.1 Asset and Risk Identification

Information assets and risks to operations will be identified during annual meetings, by the Group Risk Manager (fulfilled by the Group Chief Executive Officer), and interviews with key business managers (Operational Management, IT Management, Financial Management, HR Management) and process owners within the Digicall Group. The IT Infrastructure Manager or his/her team documents the assets within an information asset list or risk register. Where possible/appropriate, information assets are grouped together to simplify the management of the risk and compliance.

The asset list must contain at a minimum:

1. A name and description of the asset/risk.
2. The physical and/or logical location of the asset. This may include an application or system.
3. The type of asset/risk.
4. The employee/interviewee that described the asset.
5. The Owner of the asset/asset group

4.2 Asset Owners

Owners of the assets/asset groups are identified and documented in the asset/risk register. The owner is defined as an individual with overall responsibility for ensuring appropriate security and control is applied to the assets.

Note: The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ’owner’ does not mean that the person has any property rights to the asset.

4.3 Business Impact Assessment

In identifying the list of risks to IT services, what is important for the Digicall Group is the degree and severity of the impact of that service failing or operating at a non-optimized level. The Digicall Group approach to risk will ensure that full analysis is made of the potential impact to the business of these risks being realized. This will be performed by the Group Risk Manager.

4.4 Risk Assessment

The current state of the organization is assessed against each risk/threat, based on information from the interviews and assessment, specific risk assessment meetings, and information obtained in the risk assessment process.

The Risk Assessment calculates the overall risk value to the asset/groups and details a risk rating to help the organization identify high risks and exposures. Appropriate management action must then be taken to assess the appropriate action to mitigate the risk, or to accept, transfer or avoid the risk.

4.4.1 Measurement of Risk

The Digicall Group uses a straightforward combination of impact, likelihood, and the effectiveness of controls to judge the overall level of risk. To enable the Digicall Group to prioritize the mitigations to threats to their interests, the IT Infrastructure Manager together with subject matter experts are empowered to rate the importance of the threat in accordance with the following Impact Assessment table:

Impact

Impact factor	Financial	Continuity of supply	Rating
Catastrophic	Significant cost overruns of >20% over budget. Effect on revenue / asset base of >10%.	Risk event will result in widespread and lengthy reduction in continuity of supply to customers of greater than 72 hours	100%
Critical	Major cost overruns of between 10% & 20% over budget. Effect on revenue / asset base of between 5% & 10%	Reduction in supply or disruption for a period ranging between 48 & 72 hours over a significant area	70%
Serious	Moderate impact on revenue and assets base	Reduction in supply or disruption for a period between 24 & 48 hours over a regional area	50%
Significant	Minor impact on revenue and assets base	Brief local inconvenience (work around possible). Loss of an asset with minor impact on operations	30%
Minor	Insignificant monetary loss	No impact on business or core systems	10%

4.4.2 Likelihood Assessment

For each threat, the organizations' current and literal exposure is assessed, based on the controls currently in place, information obtained from interviews, knowledge of the business and processes, to determine the potential impact to the business if the risk/threat were realized. The IT Infrastructure Manager along with subject matter experts will select a likelihood rating for each risk based on the following table:

Likelihood

Almost Certain	The risk is almost certain to occur in the current circumstances	90%
Likely	More than an even chance of occurring	65%
Unlikely	Small likelihood but could happen	30%
Rare	Not expected to happen - Event would be a surprise	10%

4.4.3 Risk Analysis

The risk measure is calculated by multiplying the impact value of the asset/asset group by the likelihood of the risk happening. To calculate the Inherent Risk, the following calculation is performed:

Likelihood x Impact = Inherent Risk

Inherent Risk		**Calculation**
Extreme	≥ 50	Impact % x Likelihood %
High	≥ 35 < 50	
Moderate	≥ 25 < 35	
Low	≥ 15 < 25	
Insignificant	< 15	

4.4.4 Risk Management Scale

To identify the identify risk management options we need to identify the Effectiveness of Controls using the table below:

Effectiveness of controls

Very Good	Risk exposure is effectively controlled and managed.	90%
Good	Majority of risk exposure is effectively controlled and managed.	80%
Satisfactory	There is room for some improvement	65%
Weak	Some of the risk exposure appears to be controlled, but there are major deficiencies	40%
Unsatisfactory	Control measures are ineffective	20%

The Residual Risk rating is then calculated using the below calculation:

Priority / residual risk		**Calculation**
Priority 1	≥ 25	Inherent risk (1 - Effectiveness %)
Priority 2	≥ 17.5 < 25	
Priority 3	≥ 12.5 < 17.5	
Priority 4	≥ 7.5 < 12.5	
Priority 5	< 7.5	

The Risk Assessment must detail the resulting Risk Value for each identified theme.

4.5 Risk Treatment

1. All risks that result in a Priority 4 or Priority 5 risk measure will automatically be accepted and no further action will be required.

2. All Risks that result in a Priority 3, Priority 2 or Priority 1 will be reviewed for further management action. The IT Infrastructure Manager will review all such risks with the Asset Owners to decide an appropriate risk treatment action.

4.6 IT Risk Register and Treatment Plan

The IT Infrastructure Manager is responsible for establishing and maintaining the IT Risk Register to achieve the identified control objectives.

The risk treatment plan will identify priorities based upon the perceived risk, and considers funding, responsibilities, actions, and estimated date of completion.

The IT Infrastructure Manager is responsible for tracking and chasing the progress of risk treatments and updating the Risk Treatment Plan with progress and updated actions.

The IT Infrastructure Manager will review the IT Risk Register and Treatment Plan quarterly as part of the Management Reviews and ensure that actions are being implemented and significant risks are reported.

4.7 Ongoing Risk Management

The ongoing management of risks is controlled by accessing data from incident reports, audit results, technical advisories and confirmed or potential technical or process vulnerabilities and if required creating subsequent risk assessments. New critical information assets, processing facilities and buildings are subjected to risk assessment as part of the project process.

The IT Infrastructure Manager is responsible for ensuring that changes to the Digicall Group, its technology, business objectives, processes, legal requirements and identified threats are incorporated into the Risk Assessment and Management process. Where appropriate the IT Infrastructure Manager will initiate a risk assessment process to ensure that security controls are relevant. The risk assessment must follow the same assessment process detailed in this document.

The Digicall Group can, if required, reactively implement additional controls without undertaking a full risk assessment, if the threat or vulnerability could have a significant impact on the Digicall Group, its partners, or personnel.

5 Responsibilities

The IT Security and Compliance Manager is responsible for maintaining this policy and providing support and advice during its implementation in line with the IT Risk Management Policy

All Managers are personally responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

6 Policy Compliance Monitoring

6.1 Compliance

Group IT will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

If any user is found to have breached this policy, they may be subject to the Digicall Group's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

6.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

6.3 Non-compliance

All users (employees, contractors, vendors) are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

6.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity, criticality, and impact, opportunities may be provided to correct identified non-compliance. This corrective action will be evaluated on a case-by-case basis and timelines will be imposed and strictly enforced to ensure timeous remediation.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Human Resources Department or the IT Security and Compliance Officer.

7 Policy Governance

The following table identifies who within the Digicall Group is **Accountable, Responsible, Informed** or **Consulted** with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IT Security and Compliance Manager
Accountable	Group Chief Information Officer
Consulted	IT Infrastructure Manager, Regional IT Infrastructure Managers
Informed	All Employees, All Temporary Staff, All Contractors, All Vendors and All Suppliers

8 Audit and Review Process

This policy and compliance there to, will be audited and reviewed internally at least once every 12 months depending on the changes or requirements within the group which will be reviewed by Management, or as required by significant changes in business operations or regulatory requirements.

For Group companies' pursuing certification, policies are required to be audited externally at least once in a 36-month cycle or sooner depending on changes or requirements within the group. Any employees or contractors with suggestions should refer these to their line manager in the first instance so they can be considered for implementation. Whenever changes are made to this policy the final draft will be shared with the Group CIO, IT Infrastructure Manager and the IT Security & Compliance Manager for review and approval before publication.

The IT Security and Compliance Manager will undertake annual policy reviews.

9 Appendices

IT Risk Register and Treatment Plan.