Integrated Management System Policy

CONFIDENTIALITY
No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of CWG Plc. This document, its associated appendices and any attachments remain the property of CWG Plc and shall be returned upon request

Document History

Prepared By	Version	Date	Signature	Comment
Marcel Odiboh	2.0	15/04/2020	M.O.	Second Version

Document Approval / Review

	Name	Designation	Signature	Date
Reviewed	Oluwabunmi Adewunmi	ISMS Manager	O.E.A.	22/04/2020
Reviewed	Olatunji Aduloju	BCMS Manager	O.A.	22/04/2020
Approved	Ireti Yusuf	VP, Service Delivery	M.I.	27/04/2020
Approved	Adewale Adeyipo	CEO	A.A.	05/06/2020

Distribution

Name	Date
All Staff	05/06/2020

Change Control

The contents of this document are subject to change control

Contents

1 Introduction

This policy defines how Information Security (ISO 27001:2013) and Business Continuity (ISO 23001:2012) will be set up, managed, measured, reported on and developed within CWG.

CWG has decided to pursue full certification to ISO/IEC 27001 and ISO 22301 in order that the effective adoption of information security and Business continuity best practice may be validated by an external third party.

IMS Policy

1.1 Scope of the IMS

For the purposes of certification within CWG, the boundaries of the Integrated Management System are defined in the IMS Context Requirements Scope Document:

1.2 Integrated Management System Requirements (IMS)

A clear definition of the requirements for IMS will be agreed and maintained with the business so that all ISMS and BCMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements with regard to the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the CWG Integrated Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

1.3 Top Management Leadership and Commitment

Commitment to information security and Business continuity extends to senior levels of the organization and will be demonstrated through this IMS Policy and the provision of appropriate resources to provide and develop the IMS and associated controls.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality objectives are being met and quality issues are identified through the audit programme and management processes. Management Review can take several forms including departmental and other management meetings.

The IMS Manager shall have overall authority and responsibility for the implementation and management of the Information Security and Business Continuity Management Systems, specifically:

- The identification, documentation and fulfilment of IMS requirements
- Implementation, management and improvement of risk management processes
- Integration of processes
- Compliance with statutory, regulatory and contractual requirements
- Reporting to top management on performance and improvement

1.4 Framework for Setting Objectives and Policy

An annual cycle will be used for the setting of objectives for the Integrated Management System, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the annual management review with stakeholders.

IMS objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on an annual basis to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001:2013 the control objectives and policy statements detailed in Annex A and the ISO 22301 standard will be adopted where appropriate by CWG. These will be reviewed on a regular basis in the light of the outcome from risk assessments and BIA and in line with IMS06004 Information Security Risk Treatment Plan and procedure for conducting the Business impact Analysis. For references to the controls that implement each of the policy statements given please see IMS Statement of Applicability. See the CWG-IMS-0401 Context and Scope Document for the IMS Objectives.

1.5 Roles and Responsibilities

Within the field of information security and business continuity, there are a number of management roles that correspond to the areas defined within the scope set out above. In a larger organization, these roles will often be filled by an individual in each area. In a smaller organization these roles and responsibilities must be allocated between the members of the team.

Full details of the responsibilities associated with each of the roles and how they are allocated within CWG are given in a separate document CWG-IMS-0502, IMS Roles and Responsibilities.

It is the responsibility of the IMS Manager to ensure that staff understand the roles they are fulfilling and that they have appropriate skills and competence to do so.

1.6 Continual Improvement Policy

CWG policy about Continual Improvement is to:

- Continually improve the effectiveness of the IMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001/22301
- Achieve ISO/IEC 27001/22301 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) about information security

- To create an information security resilient organization that supports physical security features for all clients
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- To create a well-documented business continuity plan and business continuity management system for CWG Plc.
- Preserve the ability to meet stakeholder expectations in a wide range of circumstances, including meeting 3rd party arrangements
- Obtain ideas for improvement via regular meetings with stakeholders and document them in a Continual Improvement log
- Review the Continual Improvement Plan at regular management meetings in order to prioritise and assess timescales and benefits
- To protect critical information assets and critical business processes relative to CWG Plc core business

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments, Business Impact analysis and service reports. Once identified they will be added to the Continual Improvement Log and evaluated by the staff member responsible for Continual Service Improvement.

As part of the evaluation of proposed improvements, the following criteria will be used:

- Cost
- Business Benefit
- Risk
- Implementation timescale
- Resource requirement

If accepted, the improvement proposal will be prioritised in order to allow more effective planning.

1.7 Approach to Managing Risk

Risk management will take place at several levels within the IMS, including:

- Management planning – risks to the achievement of objectives
- Information security and IT service continuity risk assessments
- Business Impact Analysis
- Assessment of the risk of changes via the change management process
- As part of the design and transition of new or changed services
- Risk to Critical Business Processes

High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision.

1.7.1 Risk Assessment Process

A risk assessment process will be used which is line with the requirements and recommendations of ISO/IEC 27001, the International Standard for Information Security. This is documented in ISMS Risk Assessment and Treatment Process.

From this analysis, a risk assessment report will be generated followed by a risk treatment plan. This will then give rise to the selection of appropriate controls. Appropriate risk assessment and treatment Method would be applied for processes and activities for the Business continuity Management System.

1.8 Human Resources

CWG will ensure that all staff involved in IMS are competent based on appropriate education, training, skills and experience.

The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill levels within CWG. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

Training, education and other relevant records will be kept by the HR Department to document individual skill levels attained.

1.9 Auditing and Review

Once in place, it is vital that regular reviews take place of how well information security and Business continuity processes and procedures are being adhered to. This will happen at three levels:

1. Structured regular management review of conformity to policies and procedures – done during management review meetings at least once annually

2. Internal audit reviews against the ISO/IEC 27001/22301 standard by the CWG Internal control Team

3. External audit against the standard in order to gain and maintain certification.

1.10 Documentation Structure and Policy

All IMS policies and plans must be documented. This section sets out the main documents that must be maintained in each area.

Details of documentation conventions and standards are given in the IMS07002 Procedure for the Control of Documented Information.

Several core documents have been created and will be maintained as part of the IMS. They are uniquely numbered, and the current versions are tracked in IMS07001 IMS Documentation Log.

1.11 Control of Records

The keeping of records is a fundamental part of the IMS. Records are key information resources and represent evidence that processes are being carried out effectively.

The controls in place to manage records are defined in the document CWG-IMS-0702, IMS Procedure for the Control of Records.