INFOSEC SYSTEM - INTERNAL
ISO/IEC 27001
Information Security Management Systems Policy

Version 1.0

Created by:	Matt Thompsett
Filename:	GLC_ISO27001_Policy Document_v1.0_Client.docx
Published:	Thursday, August 9, 2018

Green Lemon Company Ltd |Mocatta House | Trafalgar Pl | Brighton | BN1 4DU
Tel +44 (0) 1273 006033

TABLE OF CONTENTS

DOCUMENT MANAGEMENT

Document Owner:

Name	Position	Responsible For	System Role
Matt Thompsett	CEO	Contents	Executive Sponsor

Document Approval

Name	Position	Authorised Signatory	System Role
Jon Idle	COO	Yes	Oversight
Nick Hines	CTO	Yes	Oversight/Audit

0 INTRODUCTION

0.1 General

In 2017 by committing to an enhanced security strategy, the GLC board decided to use The International Standard ISO/IEC 27001 as the chosen model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

The adoption of an ISMS is a key strategic decision for GLC. The design and implementation of an organisation's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organisation, hence our ISMS is designed to be robust but open to continuous and never-ending improvement involving staff at all levels. As GLC continues to enjoy success and rapid growth, our ISMS will mature and evolve to map onto our InfoSec requirements.

GLC's supporting systems and service offerings will change over time. It is expected that our ISMS implementation will be scaled in accordance with the needs of the organisation. We expect that our ISMS will come under scrutiny form many interested parties; suppliers, clients, procurement teams etc, hence we invite everyone at GLC to input to, work within and embrace our ISMS to the benefit of us all.

We plan to achieve formal certification against the International Standard by the Q3 2019, in the meantime we will work to the standard and its requirements.

0.2 Process Approach

This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving our ISMS. Any organisation needs to identify and manage many activities in order to function effectively.

All activities using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process. The application of a system of processes within an organisation, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach". The process approach for information security management presented in the International Standard encourages us to emphasise the importance of:

- understanding an organisation's information security requirements and the need to establish policy and objectives for information security;
- implementing and operating controls to manage an organisation 's information security risks in the context of the organisation's overall business risks;
- monitoring and reviewing the performance and effectiveness of the ISMS; and
- continual improvement based on objective measurement.

We have adopted the standard's "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes.

Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations.

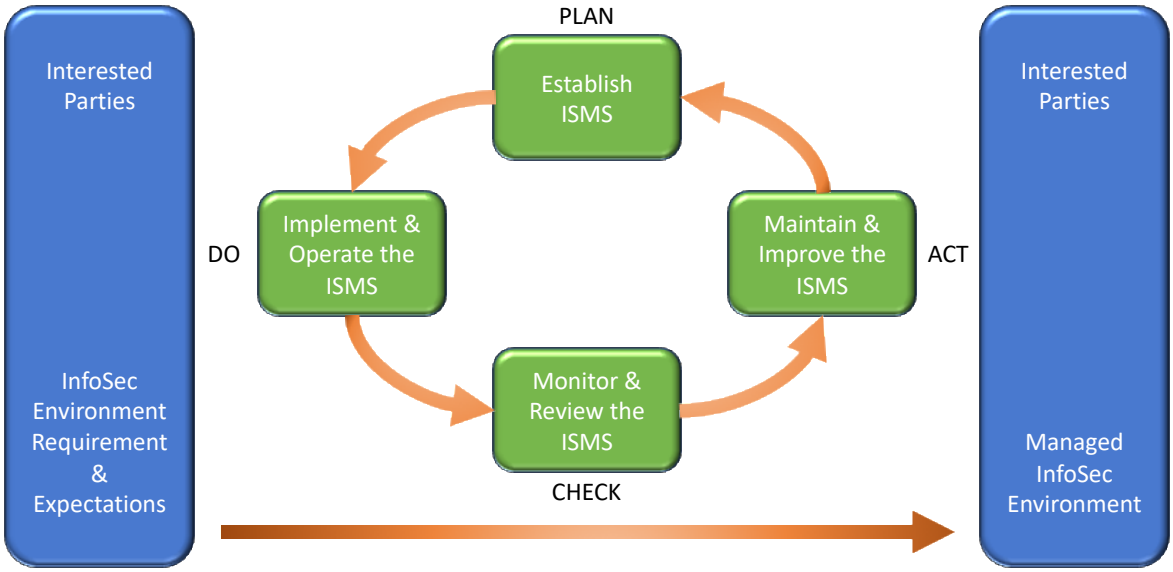

Figure 1 — PDCA model applied to ISMS processes

0.2.1 Plan (establish the ISMS)

Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation's overall policies and objectives.

0.2.2 Do (implement and operate the ISMS)

Implement and operate the ISMS policy, controls, processes and procedures.

0.2.3 Check (monitor and review the ISMS)

Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

0.2.4 Act (maintain and improve the ISMS)

Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8. The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)1) governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

0.3 Compatibility with other Management Systems

ISO/IEC 27001 is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards.

1 SCOPE

1.1 General

The standard covers all types of organisations (e.g. commercial enterprises, government agencies, non-profit organisations). The standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks.

It specifies requirements for the implementation of security controls customised to the needs of individual organisations or parts thereof. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

GLC, as a reseller and services provider, has a relatively simple engagement process. We do not;

a) process or control data on behalf of clients or their customers;

b) store client or customer data for any other purpose than development and testing;

c) provide access control or credential services;

d) do not host client systems or infrastructure (we work with our platform providers who provide infrastructure when required behind their security systems/processes); or

e) host, manage or control transactions involving client data.

1.2 Application

The requirements of the standard are generic; hence we are not able to claim any exclusions from any of the requirements specified if we wish to claim conformity to the International Standard. This may mean that conformance with some of the requirements may seem onerous or somewhat unnecessary at this time, however our efforts will be a solid investment for the future.

2 NORMATIVE REFERENCES

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management ISO/IEC 27001:2005(E) 2 © ISO/IEC 2005 – All rights reserved

3 TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions extract from the standard apply;

3.1 Asset

anything that has value to the organisation [ISO/IEC 13335-1:2004]

3.2 Availability

the property of being accessible and usable upon demand by an authorised entity [ISO/IEC 13335-1:2004]

3.3 Confidentiality

the property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO/IEC 13335-1:2004]

3.4 Information Security

preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved [ISO/IEC 17799:2005]

3.5 Information Security Event

an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [ISO/IEC TR 18044:2004]

3.6 Information Security Incident

a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC TR 18044:2004]

3.7 Information Security Management System ISMS

that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.8 Integrity

the property of safeguarding the accuracy and completeness of assets [ISO/IEC 13335-1:2004]

3.9 Residual Risk

the risk remaining after risk treatment [ISO/IEC Guide 73:2002] ISO/IEC 27001:2005(E) © ISO/IEC 2005 – All rights reserved

3.10 Risk Acceptance

decision to accept a risk [ISO/IEC Guide 73:2002]

3.11 Risk Analysis

systematic use of information to identify sources and to estimate the risk [ISO/IEC Guide 73:2002]

3.12 Risk Assessment

overall process of risk analysis and risk evaluation [ISO/IEC Guide 73:2002]

3.13 Risk Evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of the risk [ISO/IEC Guide 73:2002]

3.14 Risk Management

coordinated activities to direct and control an organisation with regard to risk [ISO/IEC Guide 73:2002]

3.15 Risk Treatment

process of selection and implementation of measures to modify risk [ISO/IEC Guide 73:2002] NOTE: In this International Standard the term ‘control’ is used as a synonym for ‘measure’.

3.16 Statement of Applicability

documented statement describing the control objectives and controls that are relevant and applicable to the organisation’s ISMS. NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organisation’s business requirements for information security.

4 INFORMATION SECURITY MANAGEMENT SYSTEM

4.1 General Requirements for the ISMS

GLC offers services and is achieving success within several sectors with a high sensitivity to Information Security, e.g. financial services. To maintain and strengthen our position and to remain competitive with our larger competitors, it is necessary for us to adopt best practice and establish a robust ISMS. The GLC InfoSec Policy shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organisation's overall business activities and the risks it faces.

For the purposes of moving forward to an International Standard certification the process used is based on the PDCA model shown in Figure 1.

4.2 Establishing and Managing the ISMS

4.2.1 Establishing GLC's ISMS

The company's ISMS is described at high-level as follows; .

f) Scope

GLC's ISMS applies without modification to all client, sales & marketing, third-party and supplier data without exception.

g) Policy

GLC's ISMS Policy is that data and other intellectual assets in all forms are to be treated as confidential and are to be used only for the intended purpose agreed between the authorised parties. Policy likewise requires that staff at all levels treat privacy and security as mandatory operating standards for the organisation and individual. GLS's Policy is described as follows:

1) Objectives

To ensure our policy meets our aspirations we have a framework (Appendix A) for setting and measuring performance against our objectives for the ISMS. The framework has broad implementation objectives set by our board supported by objectives for each aspect of the system which art the core of our PDCA model.

Staff at all levels are encouraged to input to the objectives framework and to own outcomes. The board is committed to meeting/exceeding ISMS objectives.

Our ISMS must be a dynamic and proactive strategy that not only achieves our InfoSec requirements but also promotes Continuous Improvement in processes, performance, delivery and integrity.

2) Requirements and Obligations

In every aspect of our operation proper consideration must be given to our obligations to our commercial health, legal & regulatory requirements (such as GDPR) and contractual security.

In this respect, data and assets must be profiled by our Risk Assessment Process which attributes value and risk level to guide us in establishing the most appropriate security arrangements.

Management is committed to keeping up to date in latest legislation/regulatory requirements as well as ensuring the Contractual Reviewal Process is strictly adhered to throughout client engagements.

3) Strategic Considerations

In the context with strategic risk management, GLC is a development and consultancy organisation and has no plans to take on Data Processing in any form. Our interaction with client data is solely for the purposes of application/system development in which process we are occasionally asked to work with live data.

Organisational policy is that we will try to develop solutions to avoid using live data by finding ways to use test or redacted data whenever possible. Likewise, we will not host live data on behalf of clients using our platform providers' infrastructure where necessary.

4) Risk Criteria

Our risk assessment methodology will use several criteria to provide a consistent and meaningful measure for determining security requirements. All criteria receive a score from 1-5 (1 being the lowest) for;

- Value
- Vulnerability
- Threats

5) Management Approval

GLC's ISMS has been approved by the GLC Board.

h) Risk Assessment Approach

1) Risk Assessment Methodology (RAM)

To prevent repetitive effort our RAM divides risk into two classes; General and Specific. A General risk is one that exists across the business (e.g. the use of email, office systems, BYOD, etc) whereas Specific risks tend to be client assets (e.g. Project Specifications, Test Data, Wireframes, etc).

General and Specific risks are assessed by the same methodology. General risks are managed by standing directives/work instructions, whereas Specific risks are managed by project/engagement RAID logs and project directives.

The RAM process is that each area of risk is defined and recorded on a RAM Matrix (Appendix B) and scored by a working group identified on the Matrix against the criteria in 4.2.1.b.4. The resultant score dictates the level of risk and hence the measures to be taken which range from relying on proprietary security to refusing to accept the data/asset.

To allow necessary flexibility, the working group can determine unique controls and risk treatments which are recorded on the Matrix.

RAM Matrix are reviewed according to the frequency decided by the working group and recorded on the relevant Matrix, reviews are scheduled by GLC's security officer who is also responsible for managing the process in compliance with this policy.

Management review the process once per quarter to ensure compliance with legal, regulatory and information security requirements. GLC's CTO reviews project-based RAM Matrix in accordance with the working group's decisions.

2) Acceptance of Risk

Risks may be accepted only if it is assessed that the risk score as assessed by the RAM Matrix is Low to Medium.

For each of the risks identified and accepted, following the risk assessment, a risk treatment decision needs to be made and recorded on the RAM Matrix.

Risks carrying High scores are declined where possible or mitigated by reworking, modifying, etc until a Low to Medium score is achieved.

i) Risks Within Scope of the ISMS

Asset	Owner	Threats	Vulnerabilities	Impact
Live Personal Data	Client/Customer	Proliferation via email, screen shot, download, extract Unauthorised publication Theft	Control of access Control of BYOD Remote working Storage practices Use of email Use of 3rd Party systems, e.g. Slack	Legal Regulatory Contractual Client confidence Adverse publicity
Test Data	Client			Contractual Client confidence
Project Documentation	Client			Contractual Client confidence
Client Correspondence	Client/GLC			Client confidence
Supplier Assets	Supplier			Contractual Supplier confidence
Sales & Marketing Data	GLC			Competitor advantage Business continuity
GLC Business Assets, Tools, etc	GLC			Business continuity
GLC Financials	GLC	External attack	Access control Password system	Business continuity
GLC Credentials	GLC	External attack	Password system BYOD	System Denial Business continuity

j) Risk Analyse and Evaluation, The RAM Matrix shall record:

1) an assessment of the business impacts upon the organisation that might result from security failures, considering the consequences of a loss of confidentiality, integrity or availability of the assets.

2) an assessment of the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

3) an estimate the levels of risks.

4) whether the risks are acceptable or require treatment using the criteria for accepting risks established in 4.2.1c)2).

k) Options for the Treatment of Risks, the ISMS allows us to:

1) apply appropriate controls specified in the RAM Matrix;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organisation's policies and the criteria for accepting risks (see 4.2.1c)2));

3) objectively avoid and/or decline risks; and

4) transfer the associated business risks to other parties, e.g. insurers, suppliers

All such treatments are to be recorded on the RAM Matrix and communicated to the relevant parties. All treatments should seek to remove risk or mitigate to an acceptable level.

l) Control Objectives and Controls for the Treatment of Risks

Control objectives and controls have been selected from the ISO/IEC 27001 Standard and are to be implemented to meet the requirements identified by the risk assessment and risk treatment process (Appendix C – Statement of Applicability)

m) Management Approval

Proposed residual risks defined in the RAM Matrix require management approval, such approval may be in the form of countersignature of the RAM Matrix or any other auditable method, e.g. DocuSign, email, etc.

n) Management Authorisation to Implement and Operate the ISMS

The GLC board have mandated implementation of the ISMS and recorded this authorisation in the company's board minutes.

o) Statement of Applicability

A Statement of Applicability has been prepared as Appendix C that includes the following:

1) the control objectives and controls selected and the reasons for their selection;

2) the control objectives and controls currently implemented (see 4.2.1e)2)); and

3) the exclusion of any control objectives and controls in Annex A of the ISO/IEC 27001 standard and the reason for their exclusion.

4.2.2 Implementing and Operating the ISMS

The main components of our ISMS are:

a) A Risk Treatment Plan that identifies appropriate management action, methods, resources, responsibilities and priorities for managing information security risks (Appendix D). This plan is a guide for the working groups as they work through RAM Matrix process.

b) The Risk Treatment Plan integrates with the RAM process to give guidance on meeting control objectives and give proper consideration to funding and allocation of roles and responsibilities.

c) Controls selected in 4.2.1g) to meet the control objectives.

d) Quarterly management reviews of the control measures which are graded to measure the effectiveness of the selected controls these grades are to be used to assess control effectiveness in producing comparable and reproducible results.

e) Training and awareness programmes (see 5.2.2).

f) Management oversight of the operation of the ISMS.

g) Resources assigned to the ISMS (see 5.2).

h) A process for enabling prompt detection of security events and subsequent response to security incidents (see 4.2.3a)).

4.2.3 Monitoring and Reviewal of the ISMS

Our processes are as follows:

a) We monitor and review procedures and other controls to:

1) promptly detect errors in the results of processing;

2) promptly identify attempted and successful security breaches and incidents;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) help detect security events and thereby prevent security incidents by the use of indicators; and

5) determine whether the actions taken to resolve a breach of security were effective.

This is achieved by monitoring projects as part of the Agile process otherwise according to the parameters detailed in the relevant RAM Matrix, the outcomes of these security audits are recorded on the relevant RAM Matrix.

b) We undertake quarterly reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) considering results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties. The reviews are conducted by a delegated senior manager and recorded at board meetings with associated time-bound actions.

c) We measure the effectiveness of controls to verify that security requirements have been met.

d) We review risk assessments at planned intervals as noted in 4.2.3.a and review the residual risks and the identified acceptable levels of risks, considering changes to:

1) the organisation;

2) technology;

3) business objectives and processes;

4) identified threats;

5) effectiveness of the implemented controls; and

6) external events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate.

e) We conduct quarterly internal ISMS audits which are conducted by a delegated staffer and recorded at board meetings with associated time-bound actions.

f) We ensure that the scope remains adequate and improvements in the ISMS process are identified by the process of management review (see 4.2.3.b).

g) We update security plans to consider the findings of monitoring and reviewing activities (see 4.2.3.b).

h) We record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.2.3.b).

4.2.4 Maintaining and Improving the ISMS

Our processes are as follows:

a) We implement the identified improvements in the ISMS according to the outcomes from Monitoring and Reviewal.

b) We take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. and apply the lessons learnt from the security experiences of other organisations and those of the organisation itself.

c) We communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

d) We ensure that the improvements achieve their intended objectives.

4.3 Documentation Requirements

4.3.1 General

Documentation shall include records of management decisions to ensure that actions are traceable to management decisions and policies and that the recorded results are reproducible.

For audit purposes important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

Our ISMS documentation includes, within this document or as noted:

a) documented statements of the ISMS policy (see 4.2.1b)) and objectives (Appendix A);

b) the scope of the ISMS (see 4.2.1a));

c) procedures and controls (Appendix C) in support of the ISMS;

d) a description of the risk assessment methodology (see 4.2.1c));

e) the risk assessment report (Appendix B) (see 4.2.1c) to 4.2.1g));

f) the risk treatment plan (Appendix D) (see 4.2.2b));

g) documented policies and procedures needed by the organisation to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3c));

h) records required by this International Standard (see 4.3.3); and

i) the Statement of Applicability (Appendix C).

4.3.2 Control of Documents

Documents required by the ISMS are protected and controlled. SharePoint is the sole repository for documentation either in the General Folder for generic documentation or in Project Folders for specific documentation, e.g. a project related RAM Matrix. Our procedure is as follows:

a) documents are drafted and approved by senior management for adequacy prior to issue;

b) documents are reviewed and updated, re-approved as necessary;

c) changes and version control for internal documents is managed by the SharePoint application;

d) only relevant versions of applicable documents will be available on SharePoint;

e) SharePoint ensures that documents remain available and are readily identifiable, other project collaboration tools such as Slack are used to store and socialise project documentation. Sales-related documents are likewise stored on our CRM;

f) SharePoint, Slack and our CRM have robust access controls that determine who can view, edit and share documents as determined by system users;

g) documents of external origin are identified by their unique nomenclature;

h) distribution of documents is controlled by SharePoint and other collaboration platforms as necessary, distribution by email is managed by the General RAM pertaining to the use of email;

i) SharePoint functionality prevents the unintended use of obsolete documents; and

j) Our nomenclature applies suitable identification to documents as follows;

   1) Client/Internal_Class_(Sub Class)_Description_Version_Extension

      e.g. XYZ_Widgets_SoW_Project_X v.1_DraftNPH

      e.g. GLC_ISMS_Audits_Proforma_v1.0

   2) This formal nomenclature has been recently introduced, care should be taken to check documents are valid and to rename working documents wherever possible.

4.3.3 Control of Records

Records are produced and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS in the forms prescribed in preceding sections and stored on SharePoint as controlled documents.

Records stored as part of our ISMS to meet any relevant legal or regulatory requirements and contractual obligations. Records are readily identifiable by their nomenclature as previously described.

The controls in place are as follows;

a) Identification – nomenclature (see 4.3.2.j)

b) Storage – managed and secured by SharePoint,

c) Protection - access to SharePoint and other systems mentioned is restricted to GLC users by password

d) Retrieval – managed by SharePoint and other systems

e) Retention Time – set on a case by case basis for client data and/or assets.

f) Disposition of Records – internal documents in SharePoint are managed within the functionality of the systems. Client data and/or assets are disposed of according to contractual requirements on a case by case basis

g) Records are kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS.

5 MANAGEMENT RESPONSIBILITY

5.1 Management Commitment

Management has a deep commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS demonstrated by:

a) the commitment and effort involved in establishing this ISMS policy;

b) board-level commitment and contribution to ISMS objectives and plans;

c) establishing our CEO as having overall responsibility for information security and our CTO as the overall ISMS manager;

d) communicating to the organisation the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);

f) deciding the criteria for accepting risks and the acceptable levels of risk;

g) ensuring that internal ISMS audits are conducted (see 6); and

h) conducting management reviews of the ISMS (see 7).

5.2 Resource Management

5.2.1 Provision of Resources

The organisation has committed the CTO and CEO as resources to work with staffers to:

a) establish, implement, operate, monitor, review, maintain and improve an ISMS;

b) ensure that information security procedures support the business requirements;

c) identify and address legal and regulatory requirements and contractual security obligations;

d) maintain adequate security by correct application of all implemented controls;

e) carry out reviews when necessary, and to react appropriately to the results of these reviews; and

f) where required, improve the effectiveness of the ISMS.

5.2.2 Training, Awareness and Competence

The organisation ensures that all personnel who are assigned responsibilities defined in the ISMS and/or use the ISMS are competent by:

a) understanding the necessary competencies for personnel performing work effecting or effected by the ISMS;

b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;

c) evaluating the effectiveness of the actions taken; and

d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

All staff are required to attend the ISMS training sessions as requested from time to time, attendance is recorded on personnel files and competency in respect of ISMS processes form part of employees' annual reviews. The following standards are mandatory:

a) All staff are required to complete their ISMS training within three months of joining the organisation;

b) Temporary or contract staff are required to attend an ISMS briefing prior on the first day of any engagement;

c) Refresher training is to be conducted annually;

d) Training and/or briefing sessions will be conducted in respect of significant changes to the ISMS prior to these changes going live; and

e) Re-training may be required following an incident or as the outcome of an audit where deficiencies have been identified;

GLC's CTO and CEO offer an open-door opportunity to any staff member wishing to spend time expanding their knowledge of the ISMS, dealing with specific security queries or to explore improvements to the ISMS.

6 INTERNAL ISMS AUDITS

The organisation conducts internal ISMS audits at quarterly intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

a) conform to the requirements of this International Standard and relevant legislation or regulations;

b) conform to the identified information security requirements;

c) are effectively implemented and maintained; and

d) perform as expected.

The audit programme is scheduled by the board and is managed by our CTO or a GLC staffer as delegated from time to time. The audit criteria, scope, frequency and methods are pre-defined as follows;

a) Criteria – the audit criteria is based on the PDCA model and shall demonstrable evidence of the Plan against its controls, that the Plan is being implemented as coordinated activity, that the activity is being regularly monitored and that improvements are being sought and actioned;

b) Scope – scheduled audits shall encompass all aspects of our ISMS, senior management may action a limited scope audit of a specific process, client project or procedure;

c) Frequency – scheduled audits will take place quarterly, limited scope audits will take place as needed from time to time or as result of an identified non-conformance or security issue (e.g. a breach, client complaint); and

d) Method – scheduled audits will be conducted as follows;

1) Selecting staffer/s at random to walk-through their understanding and use of the ISMS evidenced by their actions, e.g. file nomenclature, storage, patching frequency, etc;

2) Selecting General and Specific RAM Matrix to check compliance and that actions noted have been taken, e.g. Risk Treatment, mitigation, reviewal periods, etc;

3) Following up on corrective actions and improvements decisions to check they have been acted upon; and

4) Selecting a minimum of 3 client projects to check Risk Treatment Plans have been executed.

The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Staff Auditors shall not audit their own work. The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall are defined in this document.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes.

Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

7 MANAGEMENT REVIEW OF THE ISMS

7.1 General

GLC's board reviews the organisation's ISMS twice a year to ensure its continuing suitability, adequacy and effectiveness. The reviews include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews are documented by special board minutes, stored in the ISMS section of GLC's SharePoint structure and maintained by our CFO (see 4.3.3).

7.2 Review Input

The input to our managements review includes:

a) results of ISMS audits and reviews;

b) feedback from interested parties;

c) techniques, products or procedures, which could be used in the organisation to improve the ISMS performance and effectiveness;

d) status of preventive and corrective actions;

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) results from effectiveness measurements;

g) follow-up actions from previous management reviews;

h) any changes that could affect the ISMS; and

i) recommendations for improvement from staff, suppliers and clients.

7.3 Review Output

The output from our management reviews are decisions and actions related to the following.

a) Improvement of the effectiveness of the ISMS.

b) Update of the risk assessment and risk treatment plan.

c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:

1) business requirements;

2) security requirements;

3) business processes effecting the existing business requirements;

4) regulatory or legal requirements;

5) contractual obligations; and

6) levels of risk and/or criteria for accepting risks.

d) Resource needs.

e) Improvement to how the effectiveness of controls is being measured.

Following a review, any material changes to the ISMS, documentation, processes, etc will be communicated to all staff within 1 working week. Staff are expected to acquaint themselves with new versions of documents, changes to procedures etc. Management will review the implementation of any changes according to the criteria agreed pertaining to the issue at the time of the review.

8 ISMS IMPROVEMENT

8.1 Continual improvement

The organisation seeks to continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).

8.2 Corrective action

The organisation acts to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence and to mitigate impact. The procedure for corrective action is as follows:

a) Nonconformities are to be recorded on a Non-conformance Report (Appendix E);

b) A working group shall be formed to;

1) determine the causes of nonconformity;

2) evaluate and decide on actions needed for solution/mitigation;

3) evaluate and decide on actions to ensure that nonconformities do not recur;

4) determining and implementing the corrective action needed;

c) The group will record results of action taken (see 4.3.3); and

d) The group will review the corrective action taken within the timeframe recorded on the report; and

e) The group will communicate actions and findings to the relevant parties.

8.3 Preventative Action

By good training, auditing, correct use of the RAM Matrix process and application of the Risk Treatment Plan, the business is in a good position to meet the objectives of the ISMS. The basis of our systems is to determine and take action/s to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence.

Preventive actions are designed to be appropriate to the impact of the potential problems. The documented procedure for preventive action is as follows, the management team shall:

a) on the occasion of the ISMS quarterly review, identify potential nonconformities and their causes;

e.g. will a lack of staff training on the new document nomenclature standard cause nonconformance in document naming?

b) evaluate the need for action to prevent occurrence of nonconformities based on their potential impact and severity;

e.g. will poor nomenclature impact the objectives of the ISMS, compromise risk plans, cause breach, etc?

c) determine implementation plans for preventive action needed;

e.g. implement a staff refresher session on document nomenclature within 10 working days, conduct a limited scope audit 4 working weeks later

d) record the results of action taken (see 4.3.3);

e.g. training took place and 100% conformance was noted from the limited scope audit

e) conduct a review of previous preventive actions taken.

GLC's senior management stay current with regulatory changes through advisors and forums, likewise changes to projects and internal systems are oversighted by our CTO. These actions 'discover' significant changes from time to time which take priority in preventative action, for example adoption of a new internal technology system would be likely generate a need for training as a priority preventative action.

GLC staff are made aware in training sessions that action to prevent nonconformities is more cost-effective than corrective action.

9 APPENDIX A – OBJECTIVES FRAMEWORK (LIVE)

OBJECTIVES FRAMEWORK			
Goal	**Objective**	**Target**	**Measurement/Control**
Plan the ISMS	Develop strategy for InfoSec Decide on InfoSec Framework Determine risk assessment method	Complete by start of 2018 Adoption, adaption by Q2 2018 Complete by Q2 2018	Exists and understood at board level Framework adopted, communicated and mandated Exists and trialled
Implement the ISMS	Develop all policy documents and associated process, controls and documentation	Complete draft ISMS launched by Q3 2018	Exists and active
Implement RAM process, stage 1	Develop RAM Matrix for all generic risks	Complete by end of Q4 2018	Exists and deployed by priority
Implement Risk Treatment Plan	Develop Plan for all non-exceptional risks	Complete by end of Q4 2018	Exists and deployed against RAM Matrixes
Monitor ISMS	First management audit conducted and recorded	Complete by mid Q3 Next audit booked	Evidenced in records Non-conformances identified and acted on
Staff ISMS Aware	Training and awareness sessions run for all staff	Complete by mid Q3 2018 Session contents refined	Training assessed against audit outcomes
Implement RAM process, stage 2	Develop RAM Matrix for all specific risks	Complete by end of Q3 2018	Exists and deployed by priority
Organisational Risk	Overall organisational risk profile identified Insurance updated	Complete by end of 2018	Exists and understood at board level
ISMS Certification	Certification granted by external body	Complete by Q3 2019	Exists and is available for sales and marketing effort

10 APPENDIX B - RAM MATRIX (SAMPLE)

RISK ASSESSMENT METHODOLOGY MATRIX (RAM Matrix)			
Risk Class	**Nature of Risk**	**Description**	
Generic	Email systems Proliferation of copies, no version control	The use of email systems to circulate client project documents, financial and contractual and commercially sensitive documents	
Impact	**Likelihood**	**Level of Threat**	**Acceptable Risk Narrative**
Impact of proliferation is largely on working practices, time wasted in finding attachments, determining versions etc. Proliferation could lead to unauthorised access, hence impact on credibility with customers. There is a very low probability of contractual implications.	Low Email is a commonly used system for exchange and is inherently secure. Clients seem to be happy using email for info exchange and accept the risks. Hacking is unlikely.	Low Email systems are generally not targeted for contents. Email systems/users are occasionally 'hijacked' for spamming etc.	Yes The working group accepts the risk associated with email systems as the benefits outweigh the likelihood of an incident and its impact. However, email is clearly unsuitable for certain data transfer and the following Risk Treatment Plan should be applied as standard.
Risk Treatment Plan			
Event	**Action**	**Mitigation**	**Measurement/Control**
Client sending sensitive data files via email	Send client notice of risk in response Request client uses collaboration channel, encryption, Dropbox, etc Upload files to SharePoint and/or CRM and delete emails Advise client that emails have been deleted Update RAID log	Notice carries disclaimer of liability Client is advised of risk Client behaviour is modified Data is removed from our email system and secured in accordance with ISMS Email access is properly managed by password Email systems are to be set to patch automatically	Communication exists Files are stored correctly RAID log is updated Compliant process agreed between the parties and actioned
Value (1-5)	**Vulnerability (1-5)**	**Threat Rating (1-5)**	**Scoring** (<8 low, 9-45 medium, >45 high)
3	1	1	3 – LOW/ACCEPTABLE
WORKING GROUP	Matt Thompsett, Nick Hines, Howard Hardy		
REVIEWAL	Quarterly	**NEXT DATE**	1/10/2018
STORAGE	SharePoint ISMS	**NAME**	GLC_ISMS_RAMM_GENERIC_v1.0_EMAIL
CHANGES TO ISMS POLICY OR PROCESSES	None required subject to ongoing client behaviour		
AUTHORISED		**DATE**	9 August 2018

11 APPENDIX C – STATEMENT OF APPLICABILITY

Controls deemed not to apply to GLC's ISMS are highlighted in orange below with an explanation for their exception.

A.5 Security policy		
A.5.1 Information security policy **Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**		
A.5.1.1	Information security policy document	Control An information security policy document shall be approved by management and published and communicated to all employees and relevant external parties.
A.5.1.2	Review of the information security policy	Control The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6 Organization of information security		
A.6.1 Internal organization **Objective: To manage information security within the organization.**		
A.6.1.1	Management commitment to information security	Control Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
A.6.1.2	Information security co-ordination	Control Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
A.6.1.3	Allocation of information security responsibilities	Control All information security responsibilities shall be clearly defined.
A.6.1.4	Authorization process for information processing facilities	Control A management authorization process for new information processing facilities shall be defined and implemented. Not in scope of GLC operations
A.6.1.5	Confidentiality agreements	Control Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified and regularly reviewed.
A.6.1.6	Contact with authorities	Control Appropriate contacts with relevant authorities shall be maintained.
A.6.1.7	Contact with special interest groups	Control Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.8	Independent review of information security	Control

		The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
A.6.2 External parties **Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.**		
A.6.2.1	Identification of risks related to external parties	Control The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A.6.2.2	Addressing security when dealing with customers	Control All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
A.6.2.3	Addressing security in third party agreements	Control Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.
A.7 Asset management		
A.7.1 Responsibility for assets **Objective: To achieve and maintain appropriate protection of organizational assets.**		
A.7.1.1	Inventory of assets	Control All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
A.7.1.2	Ownership of assets	Control All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organization.
A.7.1.3	Acceptable use of assets	Control Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
A.7.2 Information classification **Objective: To ensure that information receives an appropriate level of protection.**		
A.7.2.1	Classification guidelines	Control Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
A.7.2.2	Information labelling and handling	Control An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
A.8 Human resources security		
A.8.1 Prior to employment [4)]		

Objective: To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.		
A.8.1.1	Roles and responsibilities	Control Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the organization's information security policy.
A.8.1.2	Screening	Control Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
A.8.1.3	Terms and conditions of employment	Control As part of their contractual obligation, employees, contractors and third-party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
A.8.2 During employment **Objective: To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.**		
A.8.2.1	Management responsibilities	Control Management shall require employees, contractors and third-party users to apply security in accordance with established policies and procedures of the organization.
A.8.2.2	Information security awareness, education and training	Control All employees of the organization and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
A.8.2.3	Disciplinary process	Control There shall be a formal disciplinary process for employees who have committed a security breach.
A.8.3 Termination or change of employment **Objective: To ensure that employees, contractors and third-party users exit an organization or change employment in an orderly manner.**		
A.8.3.1	Termination responsibilities	Control Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
A.8.3.2	Return of assets	Control All employees, contractors and third-party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
A.8.3.3	Removal of access rights	Control The access rights of all employees, contractors and third-party users to information and information processing facilities shall be removed upon

		termination of their employment, contract or agreement, or adjusted upon change.
A.9 Physical and environmental security		
A.9.1 Secure areas **Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.**		
A.9.1.1	Physical security perimeter	Control Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
A.9.1.2	Physical entry controls	Control Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
A.9.1.3	Securing offices, rooms and facilities	Control Physical security for offices, rooms, and facilities shall be designed and applied.
A.9.1.4	Protecting against external and environmental threats	Control Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. These provisions are managed by our landlords
A.9.1.5	Working in secure areas	Control Physical protection and guidelines for working in secure areas shall be designed and applied.
A.9.1.6	Public access, delivery and loading areas	Control Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. These provisions are managed by our landlords
A.9.2 Equipment security **Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.**		
A.9.2.1	Equipment siting and protection	Control Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.9.2.2	Supporting utilities	Control Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.9.2.3	Cabling security	Control Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
A.9.2.4	Equipment maintenance	Control Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.9.2.5	Security of equipment off-premises	Control

		Security shall be applied to off-site equipment considering the different risks of working outside the organization's premises.
A.9.2.6	Secure disposal or re-use of equipment	Control All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
A.9.2.7	Removal of property	Control Equipment, information or software shall not be taken off-site without prior authorization.
A.10 Communications and operations management		
A.10.1 Operational procedures and responsibilities **Objective: To ensure the correct and secure operation of information processing facilities.** **Not in scope of operations**		
A.10.1.1	Documented operating procedures	Control Operating procedures shall be documented, maintained, and made available to all users who need them.
A.10.1.2	Change management	Control Changes to information processing facilities and systems shall be controlled.
A.10.1.3	Segregation of duties	Control Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.10.1.4	Separation of development, test and operational facilities	Control Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.
A.10.2 Third party service delivery management **Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.**		
A.10.2.1	Service delivery	Control It shall be ensured that the security controls, service definitions and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third party.
A.10.2.2	Monitoring and review of third party services	Control The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
A.10.2.3	Managing changes to third party services	Control Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 System planning and acceptance **Objective: To minimize the risk of systems failures.**		
A.10.3.1	Capacity management	Control

		The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
A.10.3.2	System acceptance	Control Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 Protection against malicious and mobile code **Objective: To protect the integrity of software and information.**		
A.10.4.1	Controls against malicious code	Control Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
A.10.4.2	Controls against mobile code	Control Where the use of mobile code is authorised, the configuration shall ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code shall be prevented from executing.
A.10.5 Back-up **Objective: To maintain the integrity and availability of information and information processing facilities.**		
A.10.5.1	Information back-up	Control Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.
A.10.6 Network security management **Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.**		
A.10.6.1	Network controls	Control Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. GLC does not operate or manage a network
A.10.6.2	Security of network services	Control Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 Media handling **Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.**		
A.10.7.1	Management of removable media	Control There shall be procedures in place for the management of removable media.
A.10.7.2	Disposal of media	Control Media shall be disposed of securely and safely when no longer required, using formal procedures.
A.10.7.3	Information handling procedures	Control Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.

A.10.7.4	Security of system documentation	Control System documentation shall be protected against unauthorized access.
A.10.8 Exchange of information **Objective: To maintain the security of information and software exchanged within an organization and with any external entity.**		
A.10.8.1	Information exchange policies and procedures	Control Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
A.10.8.2	Exchange agreements	Control Agreements shall be established for the exchange of information and software between the organization and external parties.
A.10.8.3	Physical media in transit	Control Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
A.10.8.4	Electronic messaging	Control Information involved in electronic messaging shall be appropriately protected.
A.10.8.5	Business information systems	Control Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
A.10.9 **Electronic commerce services** **Objective: To ensure the security of electronic commerce services, and their secure use.** Not in scope of GLC operations		
A.10.9.1	Electronic commerce	Control Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
A.10.9.2	On-line transactions	Control Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.10.9.3	Publicly available information	Control The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 **Monitoring** **Objective: To detect unauthorized information processing activities.** Not in scope of GLC operations		
A.10.10.1	Audit logging	Control Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
A.10.10.2	Monitoring system use	Control

		Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
A.10.10.3	Protection of log information	Control Logging facilities and log information shall be protected against tampering and unauthorized access.
A.10.10.4	Administrator and operator logs	Control System administrator and system operator activities shall be logged.
A.10.10.5	Fault logging	Control Faults shall be logged, analysed, and appropriate action taken.
A.10.10.6	Clock synchronization	Control The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11 Access control		
A.11.1 Business requirement for access control **Objective: To control access to information.**		
A.11.1.1	Access control policy	Control An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A.11.2 User access management **Objective: To ensure authorised user access and to prevent unauthorized access to information systems.**		
A.11.2.1	User registration	Control There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
A.11.2.2	Privilege management	Control The allocation and use of privileges shall be restricted and controlled.
A.11.2.3	User password management	Control The allocation of passwords shall be controlled through a formal management process.
A.11.2.4	Review of user access rights	Control Management shall review users' access rights at regular intervals using a formal process.
A.11.3 User responsibilities **Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.**		
A.11.3.1	Password use	Control Users shall be required to follow good security practices in the selection and use of passwords.
A.11.3.2	Unattended user equipment	Control Users shall ensure that unattended equipment has appropriate protection.

A.11.3.3	Clear desk and clear screen policy	Control A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.11.4 Network access control **Objective: To prevent unauthorized access to networked services.**		
A.11.4.1	Policy on use of network services	Control Users shall only be provided with access to the services that they have been specifically authorized to use.
A.11.4.2	User authentication for external connections	Control Appropriate authentication methods shall be used to control access by remote users.
A.11.4.3	Equipment identification in networks	Control Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
A.11.4.4	Remote diagnostic and configuration port protection	Control Physical and logical access to diagnostic and configuration ports shall be controlled.
A.11.4.5	Segregation in networks	Control Groups of information services, users, and information systems shall be segregated on networks.
A.11.4.6	Network connection control	Control For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).
A.11.4.7	Network routing control	Control Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 Operating system access control **Objective: To prevent unauthorized access to operating systems.**		
A.11.5.1	Secure log-on procedures	Control Access to operating systems shall be controlled by a secure log-on procedure.
A.11.5.2	User identification and authentication	Control All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
A.11.5.3	Password management system	Control Systems for managing passwords shall be interactive and shall ensure quality passwords.
A.11.5.4	Use of system utilities	Control

		The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.11.5.5	Session time-out	Control Inactive sessions shall shut down after a defined period of inactivity.
A.11.5.6	Limitation of connection time	Control Restrictions on connection times shall be used to provide additional security for high-risk applications.
A.11.6 Application and information access control **Objective: To prevent unauthorized access to information held in application systems.**		
A.11.6.1	Information access restriction	Control Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
A.11.6.2	Sensitive system isolation	Control Sensitive systems shall have a dedicated (isolated) computing environment.
A.11.7 Mobile computing and teleworking **Objective: To ensure information security when using mobile computing and teleworking facilities.**		
A.11.7.1	Mobile computing and communications	Control A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
A.11.7.2	Teleworking	Control A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12 Information systems acquisition, development and maintenance		
A.12.1 Security requirements of information systems **Objective: To ensure that security is an integral part of information systems.**		
A.12.1.1	Security requirements analysis and specification	Control Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
A.12.2 Correct processing in applications **Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.**		
A.12.2.1	Input data validation	Control Data input to applications shall be validated to ensure that this data is correct and appropriate.
A.12.2.2	Control of internal processing	Control Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
A.12.2.3	Message integrity	Control Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

A.12.2.4	Output data validation	Control Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 Cryptographic controls **Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.**		
A.12.3.1	Policy on the use of cryptographic controls	Control A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.12.3.2	Key management	Control Key management shall be in place to support the organization's use of cryptographic techniques.
A.12.4 Security of system files **Objective: To ensure the security of system files.**		
A.12.4.1	Control of operational software	Control There shall be procedures in place to control the installation of software on operational systems.
A.12.4.2	Protection of system test data	Control Test data shall be selected carefully, protected and controlled.
A.12.4.3	Access control to program source code	Control Access to program source code shall be restricted.
A.12.5 Security in development and support processes **Objective: To maintain the security of application system software and information.**		
A.12.5.1	Change control procedures	Control The implementation of changes shall be controlled by the use of formal change control procedures.
A.12.5.2	Technical review of applications after operating system changes	Control When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.12.5.3	Restrictions on changes to software packages	Control Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
A.12.5.4	Information leakage	Control Opportunities for information leakage shall be prevented.
A.12.5.5	Outsourced software development	Control Outsourced software development shall be supervised and monitored by the organization.
A.12.6 Technical Vulnerability Management **Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.**		
A.12.6.1	Control of technical vulnerabilities	Control

		Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
A.13 Information security incident management		
A.13.1 Reporting information security events and weaknesses **Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.**		
A.13.1.1	Reporting information security events	Control Information security events shall be reported through appropriate management channels as quickly as possible.
A.13.1.2	Reporting security weaknesses	Control All employees, contractors and third-party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
A.13.2 Management of information security incidents and improvements **Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.**		
A.13.2.1	Responsibilities and procedures	Control Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
A.13.2.2	Learning from information security incidents	Control There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
A.13.2.3	Collection of evidence	Control Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
A.14 Business continuity management		
A.14.1 Information security aspects of business continuity management **Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**		
A.14.1.1	Including information security in the business continuity management process	Control A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.
A.14.1.2	Business continuity and risk assessment	Control Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
A.14.1.3	Developing and implementing continuity plans including information security	Control Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

A.14.1.4	Business continuity planning framework	Control A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	Control Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.
A.15 Compliance		
A.15.1 Compliance with legal requirements **Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.**		
A.15.1.1	Identification of applicable legislation	Control All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
A.15.1.2	Intellectual property rights (IPR)	Control Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
A.15.1.3	Protection of organizational records	Control Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
A.15.1.4	Data protection and privacy of personal information	Control Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
A.15.1.5	Prevention of misuse of information processing facilities	Control Users shall be deterred from using information processing facilities for unauthorized purposes.
A.15.1.6	Regulation of cryptographic controls	Control Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 Compliance with security policies and standards, and technical compliance **Objective: To ensure compliance of systems with organizational security policies and standards.**		
A.15.2.1	Compliance with security policies and standards	Control Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
A.15.2.2	Technical compliance checking	Control Information systems shall be regularly checked for compliance with security implementation standards.
A.15.3 Information systems audit considerations **Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.**		

A.15.3.1	Information systems audit controls	Control Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
A.15.3.2	Protection of information systems audit tools	Control Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

12 APPENDIX D - RISK TREATMENT PLAN (LIVE)

RISK TREATMENT PLAN				
Level	**Management Actions**	**Methods**	**Resources/Responsibilities**	**Priorities**
Low	Ensure RAM Matrixes completed Seek improvements in working practices Ensure risks are not elevated by changes in frequency, regulations, legal, contractual changes etc Delegate responsibility to staffers	Specified in RAM Matrixes for Generic and Specific risks e.g. modifying client behaviour, communication, offering alternatives, etc	Employees to participate in working groups Management authorisation required	Client engagement ISMS Compliance
Medium	Ensure RAM Matrixes completed, and actions reviewed Seek improvements in working practices Ensure risks are not elevated by changes in frequency, regulations, legal, contractual changes etc	Specified in RAM Matrixes for Generic and Specific risks e.g. escalating client behaviour, communicating offset liability, implementing contractual reqs, declining data exchange method, etc Projects RAID log to be upgraded Limited scope audit to be actioned	Employees and management to participate in working groups Management authorisation required CTO may oversight risk acceptance Staff should escalate issue to management	Mitigation of risk Liability offset to client Escalation ISMS compliance
High	Ensure RAM Matrixes completed, and actions reviewed Management must develop the risk acceptance case for the board	Specified in RAM Matrixes for Generic and Specific risks e.g. escalation to key stakeholders, official notice of risk, refusing project/s, implementing contractual halt, emergency audit, etc	Board authorisation mandatory Board to oversight risk acceptance Staff must escalate issue to management	Risk acceptance decision Impact analysis

13 APPENDIX E - NON-CONFORMANCE REPORT (SAMPLE)

NON-CONFORMANCE REPORT			
ISMS Component	**Specific Area**	**Description**	
Audit Process	Records	Due to workload, the auditor failed to complete the audit record. This oversight was only noticed on the subsequent audit. Hence, two NCs; failure to record in line with section 8.2 and failure to notice the missing record in line with section 4.2	
Cause	**Resolution**	**Preventative Action**	**Improvement to ISMS**
Primary cause was a lack of time to complete the audit record Secondary cause is a lack of understanding of the importance of auditing in improving the ISMS.	The audit record is to be completed by the auditor by end of Q3	A staff session on the importance of the audit process has been organised and scheduled A communication has been sent to all staff asking for ideas on how to shorten the record process	The working group suggests that records are generated as check lists that record exceptions only which are captured on non-conformance reports This suggestion has been drafted for approval by the board
WORKING GROUP	Nick Hines, Howard Hardy		
REVIEW ACTIONS	End Q3	**COMPLETE**	YES/NO
STORAGE	SharePoint ISMS	**NAME**	GLS_ISMS_NCR_AUDIT_9.8_RECORDS
AUTHORISED		**DATE**	9 August 2018