C&G Group ICT Policy

Information and Communication Technology (ICT) office

Last Updated: Oct, 2018

C&G Company Limited

Revision History

Author	Change Reference	Version	Date
Gilbert Mutai	Working Draft	1	10/18/2018
	Stakeholder Review and Revision	1	10/28/2018
	Revised Draft	1	01/10/2018

Approval History

Approver	Department	Business Title	Version	Date
Titus Murage	**ICT**	**Group Commercial manaegr**	**1**	**Oct 2018**

Standards Update Summary:

Controls Updated	Version	Updated By	Date

Table of Contents

Introduction

Purpose

C&G Information Security Policy requires protection of the company's information technology, brand, intellectual property, personal information and customer information from misuse or compromise. C&G business functions rely upon the confidentiality, integrity and availability of its information systems and the information assets stored within them. These Information Security Standards support the stated policy objectives and define Information Security requirements to meet those objectives. C&G has defined the following thirteen (13) Information Security Standards:

Information Security Standards	Brief Description
Organization of Information Security Standard	• This Information Security Standard is established to manage Information Security within C&G. The standard will provide Information Security requirements to initiate and control the implementation and operation of Information Security within C&G. It includes requirements in the following areas: ○ Security roles and responsibilities ○ Segregation of duties ○ Contacting authorities and special interest groups
Human Resources Security Standard	• This Information Security Standard is established to ensure that employees, contractors and third party users understand their responsibilities, adhere to C&G Information Security policies and standards and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. It includes requirements in the following areas: ○ Screening of employees, third-parties and contractors ○ Terms and conditions of employment ○ Security awareness, education and training ○ Disciplinary process ○ Termination and change of employment
Asset Management Security Standard	• This Information Security Standard is established to identify assets, classify and label assets and achieve and maintain appropriate protection of those assets. It includes requirements in the following areas: ○ Asset inventory ○ Asset ownership ○ Acceptable use of C&G assets ○ Return of C&G assets ○ Classification of C&G information ○ Labeling of C&G information ○ Management of removable media ○ Disposal of media ○ Physical media transfer
Logical Access Control Security Standard	• This Information Security Standard is established to control access (both privileged and non-privileged) to information, networks and C&G assets. It includes requirements in the following areas: ○ Logical access control requirements ○ Logical Access to Network and Network Services ○ Use of utility programs

	○ User registration and de-registration ○ User access authorization ○ Management of privileged access rights ○ Management of Secret Authentication Information ○ Review of user access rights ○ Removal and adjustment of access rights ○ Logical authentication procedures
Cryptography Security Standard	• This Information Security Standard is established to ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of C&G information. It includes requirements in the following areas: ○ Usage of Cryptography ○ Key Management
Physical and Environment Security Standard	• This Information Security Standard is established to prevent unauthorized physical access, damage, and interference to C&G premises and information. It includes requirements in the following areas: ○ Securing physical areas through perimeter controls, entry controls, secure offices, protecting against environmental threats etc. ○ Securing equipment – e.g. cabling security, maintenance, removal, disposal of equipment.
Operations Security Standard	• This Information Security Standard is established to ensure the correct and secure operation of information processing facilities. It includes requirements in the following areas: ○ Standard operating procedures ○ Change management ○ Capacity management ○ Separation of Security Zones ○ Protection against malware ○ Backup ○ Logging ○ Protection of log information ○ Clock synchronization ○ Installation of software ○ Management of technical vulnerabilities ○ Controlling the use of audit activities ○ Controls specific to mobile devices ○ Teleworking
Communications Security Standard	• This Information Security Standard is established to ensure the correct and secure communications of information processing facilities. It includes requirements in the following areas: ○ Network security controls ○ Security of network services ○ Segregation of networks ○ Information transfer procedures ○ Agreements on information transfer ○ Confidentiality or non-disclosure agreements

Information System Lifecycle Security Standard

- This Information Security Standard is established to ensure that Information Security is an integral part of information systems across the entire application lifecycle. This also includes Information Security requirements for information systems that undergo changes and information systems that provide services over external networks. It includes requirements in the following areas:
  - Information security requirements analysis and specification (i.e. requirements for incorporating security for new information systems or changes to existing information systems)
  - Securing application services
  - Protecting application services transactions (usage of electronic signatures, trusted authority, etc.)
  - Secure development
  - System change control procedures
  - Technical review of changes
  - Restriction on changes to software packages
  - Secure system engineering principles
  - Outsourced development
  - System security testing
  - System acceptance testing
  - Protection of test data

Supplier Relationships Security Standard

- This Information Security Standard is established for the protection of C&G information that is accessible by suppliers (third-parties, vendors, business partners, other external entities) and includes requirements in the following areas:
  - Security requirements for supplier relationships
  - Addressing security with agreements
  - Monitoring and review of supplier services
  - Managing changes to supplier services

Incident Management Security Standard

- This Information Security Standard is established to ensure Information Security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. It includes requirements in the following areas:
  - Incident management responsibilities and procedures
  - Reporting Information Security events
  - Reporting Information Security weaknesses
  - Assessment of Information Security events
  - Incident response
  - Learning from Information Security incidents
  - Collection of evidence

Information Security Continuity Security Standard

- This Information Security standard is established to define roles, responsibilities and requirements to mitigate the impact of interruptions to business activities and to protect critical business processes from the effects of major failures of information systems and/or significant events which threaten normal business operations, and to ensure Information Security continuity and/or resumption within accepted operational and business requirements. It includes requirements in the following areas:
  - Planning Information Security continuity

	○ Implementing Information Security continuity ○ Verify, review and evaluate Information Security continuity ○ Availability of information processing facilities
Compliance Security Standard	• This Information Security Standard is established to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any Information Security requirements. It includes requirements in the following areas: ○ Identification of applicable laws and regulations ○ Intellectual property rights ○ Protection of records ○ Privacy and Personal Information ○ Regulation of cryptographic controls ○ Independent review of Information Security ○ Compliance with C&G Information Security Policy and Standards ○ Technical compliance reviews (penetration testing, vulnerability scans etc.)

Each of the above Information Security Standards has the following components:

- **Control Categories –** Similar Information Security controls are logically grouped into control categories for better organization of Information Security controls and requirements. Each Information Security control category includes control/control objective stating what is to be achieved and one or more requirements within each control.

- **Control and Control Objectives –** Each Information Security Standard contains Information Security controls with control statements defining the control objectives and multiple Information Security requirements within that control.

- **Control Owner –** Control owner is the entity accountable for the implementation and maintenance of that control.

- **Requirements –** Provides more detailed requirements to meet and support the objectives of a control.

Scope

C&G Information Security Standards apply to all employees, contractors/consultants, service providers, contingent workers, interns, suppliers, business partners and vendors (collectively referred as "C&G users") acting on behalf of C&G . These C&G Information Security Standards outline requirements for all the C&G users with access to C&G information systems, facilities or information assets. All C&G users must comply with the C&G Information Security Standards.

These Information Security Standards apply to all information systems, information processing facilities, and information assets that are owned or managed by C&G , used on or accessed from C&G networks, or information systems, information processing facilities, and information assets that are used for C&G business. These requirements do not apply to products shipped to C&G customers for on premise operations.

The requirements in these Information Security Standards shall be considered the minimum acceptable requirements for the protection of C&G information systems, facilities and information assets. These Information Security Standards sets forth expectations across C&G . Additional Information Security controls may apply to certain areas of C&G , based on business related special programs, Business Group specific or regulatory requirements. These Information Security Standards shall not be construed to limit application of more stringent requirements where justified by business needs, special programs, regulatory requirements or assessed risks.

Word Usage

Use of the words “must” or “shall” indicates requirements for implementation across all in-scope systems and against which compliance will be tested.

Use of the word “should” indicates recommendations where implementation is encouraged wherever applicable but the control may not be appropriate for all systems. The security control may be applicable in certain circumstances and as such, are not firm requirements.

Use of the word “may” indicates permissible actions but not requirements. Business/IT owners are encouraged to implement as many of the “should” controls as applicable to improve the overall security of C&G .

Roles and Responsibilities

C&G users must comply with the requirements defined in these Information Security Standards.

Business/IT owners are responsible for defining and implementing Information Security controls to meet the requirements defined in these Information Security Standards and that ensure the information systems they are responsible for are managed and operated in a secure and effective manner and meet any additional regulatory and contractual requirements based on business needs and risks. They are also responsible for ensuring that their third-parties and non-C&G personnel implement appropriate Information Security controls to meet security requirements in these Information Security Standards.

The Chief Security Officer (CSO) has the overall responsibility for the Information Security Standards, and in conjunction with the Information Security Office (ISO) will be responsible for defining, implementing, managing, monitoring and reviewing compliance with these Information Security Standards.

The ISO will assist C&G users and Business/IT owners in assessing, defining, implementing, managing and monitoring appropriate Information Security controls. The ISO may also assist Business Groups in implementing, assessing and obtaining Information Security certifications such as ISO 27001.

Corporate Risk Assurance (CRA) will audit and review the adequacy of Information Security controls in place to measure and enforce conformance with these Information Security Standards.

Exceptions

The exception process acts as the formal authorization process to bypass an information security requirement. The primary benefit is to increase visibility of risks to the enterprise and to ensure that known violations are included in the assessments of effectiveness of information security controls and existing business risks.

The objective of this Exception Process is to provide a mechanism for the identification and evaluation of risks presented by solution or actions that violate the Information Security Standards and to weigh those risks against the needs of the business. Once the identified security risk has been mitigated to an acceptable level, the business unit shall accept the residual risk.

Information Security Standard Exception Process includes the following activities:

- Once an exception is submitted, Information Security Standards Working Group and Committee reviews the requests for exception to the information security requirements based on:
    - Business impact
    - Information security risks
    - Proposed remediation plan
    - Business justification

- Once an initial review is performed, Information Security Standards Working Group and Committee make an appropriate determination to approve or deny the exception request.

- If the exception is approved, the Working Group is responsible to ensure that the exception is well-documented in the Exception Log.

- The Working Group must review the exception log on an annual basis to ensure that the exception is still valid and the residual risk has not increased beyond what was originally assumed or to determine if the residual risk can be reduced further due to changes in the environment.

For any communication regarding your Risk Acceptance request, please contact Risk and Compliance

If business needs and/or regulatory requirements require implementation of stronger Information Security controls than are listed in these Information Security Standards, Business/IT owners must comply with those regulatory requirements and implement those stronger Information Security controls in consultation with the ISO.

This page is intentionally left blank.

Information Security Standard One: Organization of Information Security Standard

Information Security Standard Objective	
This Information Security Standard is established to manage Information Security within C&G. The standard will provide security requirements to initiate and control the implementation and operation of Information Security within C&G.	
Control Categories	**Controls**
Information Security Policy and Standards *To establish and sustain Information Security Policy and Standards within C&G.*	• OI-01 Information Security Policy and Standards
Internal Organization *To establish a management framework to initiate and control the implementation of Information Security within C&G.*	• OI-02 Information Security Roles and Responsibilities • OI-03 Segregation of Duties • OI-04 Contact with Special Interest Groups • OI-05 Information Security in Project Management • OI-06 Contact with Authorities

Information Security Policy and Standards

OI-01 Information Security Policy and Standards

Information Security Policy and Standards must be defined, approved by management, published and communicated to all C&G users.

Owner	Control Mapping		
Design Owner: ISO Implementation Owner: ISO	ISO 27002: 2013 A.5.1.1 ISO 27002: 2013 A.5.1.2	PCI-DSS 12.1	NIST 800-53 AT-01 NIST 800-53 CP-01 NIST 800-53 PE-01

Last Updated: October, 2018

OI-01 Requirements

1. Information Security Policy and Standards must be approved by the ISO management, published and communicated to all employees and relevant external parties.

2. Changes to the Information Security Policy and Standards are the responsibility of the ISO. ISO is responsible for reviewing proposed changes to the Information Security Policy and Standards as necessary to address commercial, legal, and regulatory requirements applicable to C&G .

3. All changes to the Information Security Policy and Standards must be approved, before publication, using C&G policy and standards management process.

4. Information Security Policy and Standards shall be reviewed annually or when critical changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

5. Requests for updates or modifications to an existing Information Security Policy or Security Standard must be submitted to the ISO for review.

6. References and additional requirements related to this control:

6.1 C&G Information Security Policy and Standards Management Process

Internal Organization

OI-02 Information Security Roles and Responsibilities

Information Security roles and responsibilities must be defined and assigned.

Owner	Control Mapping		
Design Owner: C&G Executive Management, ISO Implementation Owner: Head of the Business Groups, C&G users	ISO-27002:2013 A.6.1.1	PCI-DSS 1.1.4 PCI-DSS 12.9.1	NIST 800-53 XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37

Last Updated: October, 2018

OI-02 Requirements

1. Roles and responsibilities for the management and administration of the Information Security program must be identified and documented.

   1.1 C&G CSO is responsible for the development, governance, oversight and support of Information and Physical Security, and Enterprise Resiliency at C&G and for supporting the identification of appropriate controls and requirements to protect C&G systems, facilities and information assets.

   1.2 C&G executive management has established the ISO organization to act as a company-wide oversight authority for management of Information and Physical Security, and Enterprise Resiliency.

   1.3 C&G ISO management has the critical responsibility of enforcing and reporting of compliance with C&G Information Security Policy and Standards throughout the company. CRA and the ISO shall be responsible for the audit and assessment of these Information Security standards established by the ISO and implemented by the respective Business Groups.

   1.4 C&G users should ensure that information systems, facilities and information assets under their responsibility are compliant with the Information Security Policy and Standards.

   1.5 Responsibilities for the protection of information systems, facilities and information assets and carrying out Information Security processes must be clearly identified, documented and made available to the ISO upon request.

   1.6 Individuals with allocated Information Security responsibilities may delegate Information Security tasks to others. However, the individuals will remain accountable and are responsible for determining whether delegated tasks have been correctly performed.

   1.7 Coordination and oversight of Information Security aspects of supplier relationships must be identified and documented.

2. All Information Security requirements shall be governed by the ISO in areas such as insurance, legal issues, human resources, IT or risk management for Information Security activities, whenever applicable.

3. The following Information Security requirements shall be met by the ISO:

1.1 The ISO will document and report non-compliance with C&G Information Security Policy and Standards, to ensure completion of committed remediation activities.

3.1 The ISO must define, document and implement methodologies and processes for an annual security risk assessment.

3.1.1 Information security risk assessment process must be defined, documented and implemented including identification of threats and vulnerabilities and resulting risks to C&G assets.

3.1.2 Information security risk assessment shall be performed on an annual basis to address changes in the threat landscape, technology evolution, IT infrastructure, and/or any critical changes impacting C&G Information Security.

3.1.3 The scope of Information Security risk assessment maybe enterprise-wide, or limited to parts of C&G , critical business services, or services where it is practical, realistic and helpful for the protection of C&G assets and information.

3.1.4 Information security risk assessment procedures may include validation of the design and or effectiveness of Information Security Policy and Standards.

3.1.5 Information security assessment must identify, quantify and prioritize risks against criteria for risk tolerance and objectives relevant to C&G as per the methodologies defined by the ISO.

3.1.6 Business groups or the ISO will be responsible to determine the appropriate management actions and priorities for implementing controls to mitigate those risks based on the results of the Information Security risk assessment.

3.1.7 Information security control implementation for risk mitigation shall bring the level of risk to an acceptable risk level as defined by management with approval with C&G Security Council as necessary.

3.1.8 ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management or equivalent Information Security framework for Information Security risk management may be leveraged for performing Information Security risk assessments. The framework or methodologies for Information Security risk assessment must be approved by the ISO.

3.2 Business groups managing IT assets shall ensure the adoption and alignment to the risk based methodology as defined by ISO on a periodic basis.

3.3 The ISO shall coordinate the implementation of Information Security controls with respective cross-Business Groups such as C&G IT, Legal, Finance and CRA (as applicable) in consultation with the heads of respective Business Groups.

3.4 The ISO and the heads of the respective Business Groups must promote Information Security education, training, and awareness for all employees and contractors.

3.5 ISO shall evaluate the report(s) received from Information Security incident monitoring tools through automated and/or manual processes. ISO will ensure appropriate actions with the respective business group to mitigate the impact of Information Security incidents in a timely manner.

4. References and additional requirements related to this control:

4.1 HR-03 Information Security Awareness, Education and Training

4.2 Security in Supplier Relationships

4.3 Risk Acceptance Process

OI-03 Segregation of Duties

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of C&G information systems, facilities and information assets.

Owner	Control Mapping		
Design Owner: Business/IT Owners Implementation Owner: Business Groups	ISO-27002:2013 A.6.1.2	PCI-DSS 7.1.2	NIST 800-53 AC-5

Last Updated: October, 2018

OI-03 Requirements

1. Segregation of duties must be implemented by Business/IT owners for reduction of risk of accidental or deliberate system or information misuse.

2. No C&G user shall be allowed to access, modify or use C&G assets without authorization or detection.

   2.1 Assignment of privileges shall be based on users' job roles and responsibilities and shall be determined by the immediate supervisor based on a need-to-know principle.

   2.2 Segregation of duties should be accomplished through logical and/or physical access controls and roles and access rights must be documented by individual information system owners.

   2.3 The business / operational groups must implement their group specific procedures to meet or exceed ISO provided requirements to address compliance with segregation of duties as it pertains to their environment.

   2.4 Segregation of duties for IT environments, applications and other information systems must be implemented in accordance with applicable laws and regulations.

3. In instances where segregation of duties is difficult (e.g. development and operational activities performed by the same teams), other compensating controls, such as monitoring of activities, audit trails and management supervision must be implemented.

4. References and additional requirements related to this control:

   4.1 Business Requirements for Logical Access Control

OI-04 Contact with Special Interest Groups

Special interest groups and other special security forums and professional association’s point of contact must be identified and maintained.

Owner	Control Mapping		
Design: ISO Implementation: ISO and Business Group	ISO-27002:2013 A.6.1.4	PCI-DSS 6.3	NIST 800-53 SA-1 NIST 800-53 SA-3 NIST 800-53 SA-4

Last Updated: October, 2018

OI-04 Requirements

1. To stay up-to-date with relevant security information and to ensure that the understanding of the Information Security environment is current and complete, the ISO and Security Risk and Compliance should consider membership in various standard bodies, pertinent professional organizations, and special interest groups or forums.

2. C&G employees responsible for Information Security as part of their day-to-day job responsibilities should consider participating and obtaining membership in special interest groups, professional associations or forums such as ISSA, OWASP, SANS, and CSA.

3. The ISO should collaborate with external entities, government/state cyber security groups, and major technology vendors to receive periodic alerts on threats, vulnerabilities and patches critical to protection of C&G information systems, facilities and information assets. Collaboration with appropriate stakeholders will follow communications protocols as established by the ISO.

4. The SIO team shall provide liaison points when dealing with Information Security incidents.

OI-05 Information Security in Project Management

Information security must be addressed in project management activities.

Owner	Control Mapping		
Design Owner: ISO, PMO Implementation Owner: Business Groups, Project Managers	ISO-27002:2013 A.6.1.4	PCI-DSS 12.9.1 PCI-DSS A.1.4	NIST 800-53 IR-6 NIST 800-53 SI-5

Last Updated: October, 2018

OI-05 Requirements

1. Information security must be integrated into C&G project management methodology to ensure that Information Security risks are identified and addressed as part of a project. Project outputs must be designed to remain compliant with information security policy.

   1.1 This requirement applies to any project regardless of its character, e.g., a project for a core business process, product development project, IT project, facility management and other supporting processes.

   1.2 IT applications shall be developed in accordance with applicable Information Security laws, regulations and standards and guidelines provided by the ISO.

2. The project management process must meet the following requirements:

   2.1 The project methodology must include Information Security objectives and criteria.

   2.2 The project methodology must involve an Information Security risk assessment at an early stage to verify necessary Information Security controls applicability.

   2.3 The project methodology must identify and document Information Security roles and responsibilities for various teams and individuals involved throughout the project lifecycle including the project output operation.

3. The ISO has to be consulted at key stages of the project (gates / checkpoints) and has the authority to stop the progress of the project if information risk management and compliance criteria are not met by the project.

4. References and additional requirements related to this control:

    4.1 Application Security Framework and Review Process

OI-06 Contact with Authorities

Appropriate contacts with relevant authorities will be identified and maintained.

Owner	Control Mapping		
Design Owner: ISO, Legal Implementation Owner: Individuals as defined by the ISO and Legal	A.6.1.5	PCI-DSS 12.9.1 PCI-DSS A.1.4	NIST 800-53 IR-6 NIST 800-53 SI-5

Last Updated: October, 2018

OI-06 Requirements

1. ISO and/or local C&G authorities must maintain appropriate contacts with relevant law enforcement and supervisory authorities, external parties and providing critical infrastructure services.

    1.1 C&G Business Groups are also recommended to develop contacts with expert security groups, other specialist security forums and with pertinent professional associations.

2. Business groups in consultation with the Legal department and the ISO shall provide a predetermined authorized list of contacts with a defined and documented set of procedures that specify the engagement of authority. Authorities in this context include but are not limited to: law enforcement, fire department, supervisory authorities, regulatory bodies, emergency services, electricity suppliers, health and safety, water suppliers, telecommunication providers etc.

    1.1 Local and global legal department must be consulted prior to notification and involvement of law enforcement and federal agencies in the event of an Information Security breach.

    1.2 Corporate Security and Safety, and Facilities Management must be involved for matters related to preventative relations with fire department, emergency dispatch centers, and other state or federal agencies which do not apply to emergency situations.

2. The SIO and IT asset owners must work in collaboration to define and document procedures to notify and/or involve external third parties supporting C&G IT infrastructure and services (for e.g. telecommunication operator, Internet Service Provider, other managed services provider), including vendor and partner entities in the event of a security incident or a security breach. This applies to security breaches or incidents occurring within C&G or where C&G assets are stored within a third party environment.

    2.1 Business groups shall assign a designated individual to act as a point of contact for third-parties providing services to them. This contact is responsible to receive or communicate the security breach with the third party and involve the appropriate ISO team as needed.

    2.2 The legal department must be consulted whenever external third-parties are involved during an Information Security incident or a breach.

3. The legal department shall define and document specific procedures to involve external forensics entities in the event of an Information Security breach requiring independent forensic analysis.

4. References and additional requirements related to this control:

   4.1 Management of Information Security Incidents and Improvements

   4.2 Information Security Continuity

This page is intentionally left blank.

Information Security Standard Two: Human Resources Security Standard

Information Security Standard Objective	
This Information Security Standard is established to ensure that employees, contractors and third party users understand their responsibilities, adhere to C&G Information Security policies and standards, are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.	
Control Categories	**Controls**
Prior to Employment *To ensure that employees, contractors and external party users understand their responsibilities and are suitable for the roles for which they are considered.*	• HR-01 Screening • HR-02 Terms and Conditions of Employment
During Employment *To ensure that employees and external party users are aware of and fulfill their Information Security responsibilities.*	• HR-03 Information Security Awareness, Education and Training • HR-04 Disciplinary Process
Termination or Change of Employment *To protect the organization's interests as part of the process of changing or terminating employment.*	• HR-05 Termination or Change of Employment Responsibilities

Prior to Employment

HR-01 Screening

Background verification checks on all candidates for employment must be carried out in accordance with the relevant laws, regulations and customs and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Owner	**Control Mapping**		
Design Owner: Human Resources Implementation Owner: Human Resources	ISO-27002:2013 A.7.1.1	PCI-DSS 12.7	NIST 800-53 PS-3

Last Updated: October, 2018

HR-01 Requirements

1. Candidates considered for employment must be adequately screened prior to employment by Human Resources.

2. Employee background verification checks shall be carried out by Human Resources (or a C&G -approved external agency) taking into account all relevant national and regional privacy, protection of personal data and/or employment based laws, government clearance requirement (if applicable) and background screening will be conducted in accordance with C&G Background Check and Drug Testing Policy.

3. Human Resources shall document procedures to define criteria and limitations for verification checks.

3.1 Human Resources shall document procedures to securely store and manage background check and application information and will retain this information in accordance with the Corporate Records Retention policy.

4. A screening process must also be carried out for contractors and third party users where permitted by local regulation and customs. For instances where contractors are employed through a recruiting firm or agency, the contract shall clearly specify the recruiting firm's or agency's responsibilities for conducting screening.

5. Information on candidates being considered for positions within C&G must be collected, handled and retained in accordance with locally applicable laws and C&G Information Systems Classification and Handling Standard, as well as C&G Global Records Management Policy and Records Retention Schedule.

6. References and additional requirements related to this control:

6.1 Background Check and Drug Testing Policy

6.2 Information Classification and Handling Standard

6.3 Global Records Management Policy

6.4 Records Retention Schedule

HR-02 Terms and Conditions of Employment

Prior to gaining access to C&G information and assets, C&G users must agree to abide by C&G code of conduct and corporate policy and standards.

Owner	Control Mapping		
Design Owner: Human Resources, Legal Implementation Owner: Human Resources, Legal	ISO-27002:2013 A.7.1.2	PCI-DSS 12.6.2	NIST 800-53 AC-20 NIST 800-53 PL-4 NIST 800-53 PS-6 NIST 800-53 PS-7

Last Updated: October, 2018

HR-02 Requirements

1. C&G users must agree (via employment offer or contract, confidentiality or non-disclosure agreement, as applicable) to comply with C&G Policies and Standards prior to being given access to facilities or information to reduce the risk of theft, fraud, or misuse of C&G information systems. These agreements may include the following as appropriate:

1.1 C&G users who are given access to non-public information must sign a confidentiality or non-disclosure agreement prior to being given access to C&G information systems, facilities and information assets.

1.2 Intellectual property and privacy consent requirements.

1.3 Responsibilities for the classification of information, management of C&G assets associated with information systems and services handled by the C&G user

1.4 Responsibilities of the C&G user for the handling of information received from other companies or external parties.

1.5 Responsibilities of C&G for the handling of personal information, including personal information created as a result of, or in the course of, employment or engagement with C&G .

1.6 Responsibilities that are extended outside C&G premises and outside normal working hours, e.g. in the case of employees working from home.

1.7 Responsibilities of the C&G user to complete mandatory security trainings.

1.8 Actions to be taken if the C&G user disregards C&G Information Security requirements.

2. Information security roles and responsibilities shall be communicated to employees or other Users when employment or engagement commences.

3. Where appropriate and defined in the employment agreement, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

4. References and additional requirements related to this control:

4.1 Responsibility of Assets

4.2 Information Classification

During Employment

HR-03 Information Security Awareness, Education and Training

C&G users must receive appropriate Information Security awareness program, education and training and regular updates in C&G Information Security Policy, Standards and Procedures, as relevant for their job function.

Owner	Control Mapping		
Design Owner: Information Security Office, Business Groups Implementation Owner: ISO, Business Groups, C&G users	ISO-27002:2013 A.7.2.1 ISO-27002:2013 A7.2.2	PCI-DSS 8.5.6 PCI-DSS 7.2.2 PCI-DSS 12.6.1 PCI-DSS 12.6.2 PCI-DSS 12.9.4 PCI-DSS 6.5	NIST 800-53 AT-2 NIST 800-53 AT-3 NIST 800-53 AT-4 NIST 800-53 CP-3 NIST 800-53 IR-2 NIST 800-53 PL-4 NIST 800-53 PS-6 NIST 800-53 PS-7 NIST 800-53 SA-9

Last Updated: October, 2018

HR-03 Requirements

1. C&G users must complete Information Security awareness training annually.

1.1 Information security awareness and training shall be completed by C&G users within 45 days of their start date.

1.2 Supervising managers must ensure that a C&G user completes and passes the Information Security training on-time.

1.3 Based on the job roles and responsibilities and criticality of the information handled by a C&G user, additional information security trainings (e.g. secure coding training) should be provided.

2. Any updates to the Information Security Policy and Standards must be communicated to C&G users by the Information Security Office.

3. Information security training compliance shall be monitored by the ISO annually and training records shall be stored in accordance with C&G Global Records Management Policy.

4. C&G must ensure that users are provided with an anonymous reporting channel to report known or suspected violations of Information Security Policy and Standards (“whistle blowing”).

5. References and additional requirements related to this control:

   5.1 Code of Conduct Policy

   5.2 Global Records Management Policy

   5.3 Records Retention Schedule

HR-04 Disciplinary Process

There must be a disciplinary process in place to take action against C&G employees who have committed an Information Security breach consistent with C&G HR disciplinary processes.

Owner	Control Mapping		
Design Owner: Human Resources Implementation Owner: Human Resources	ISO-27002:2013 A.7.2.3	N/A	NIST 800-53 PS-8

Last Updated: October, 2018

HR-04 Requirements

1. A C&G employee who violates the Information Security Policy shall be subject to disciplinary action up to and including termination of employment.

   1.1 Any individual who violates C&G Information Security Policy and Standards may also be subject to criminal prosecution and/or civil litigation under state and/or federal law.

   1.2 The decision to initiate legal action will be made in consultation by C&G Legal department.

   1.3 C&G Users who violate C&G Information Security policy may have their logical and physical access privileges revoked and/or contracts terminated, as appropriate.

2. Disciplinary processes shall adhere to the applicable regional disciplinary policies.

Termination or Change of Employment

HR-05 Termination or Change of Employment Responsibilities

Information security responsibilities and duties that remain valid after termination or change of employment must be defined, communicated to the C&G User and enforced.

Owner	Control Mapping		
Design Owner: Human Resources Implementation Owner: Human	ISO 27002:2013 A.7.3.1	PCI-DSS 7.1.1 PCI-DSS 8.5.4	NIST 800-53 PS-05

Resources, Supervising Manager			

Last Updated: October, 2018

HR-05 Requirements

1. It is the managing supervisor or sponsor’s (for a third party) responsibility to initiate appropriate physical and logical access revocation for departing C&G Users.

2. It is the users’ responsibility to report any appropriate physical or logical access privilege changes as a result of a role change to the respective manager/system administrator.

3. Information Security responsibilities and duties for the protection of C&G information after termination or change of employment must be included in the terms and condition of employment or third-party contracts. Upon termination (or change of responsibilities), affected persons may request a copy of what they agreed to when they joined.

4. References and additional requirements related to this control:

   4.1 Employee Termination Process

   4.2 Contingent Worker Termination Process

This page is intentionally left blank.

Information Security Standard Three: Asset Management Security Standard

Information Security Standard Objective	
Information Security Standard to identify assets, classify and label assets and achieve and maintain appropriate protection of those assets.	
Control Categories	**Controls**
Responsibility for Assets *To achieve and maintain appropriate protection of C&G assets.*	• AM-01 Inventory of Assets • AM-02 Ownership of Assets • AM-03 Acceptable Use of Assets • AM-04 Return of Assets
Information Classification *To ensure that information receives an appropriate level of protection in accordance with its importance to C&G .*	• AM-05 Classification of Information • AM-06 Labeling of Information • AM-07 Handling of Assets
Media Handling *To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.*	• AM-08 Management of Removable Media • AM-09 Disposal of Media • AM-10 Physical Media Transfer

Responsibility for Assets

AM-01 Inventory of Assets

Assets associated with information and information processing facilities must be identified and an inventory of these assets must be drawn up and maintained.

Owner	**Control Mapping**		
Design Owner: Business/IT Owner Implementation Owner: Business/IT Owner	ISO-27002:2013 A.8.1.1	PCI-DSS 9.9.1 PCI-DSS 12.3.3 PCI-DSS 12.3.7	NIST 800-53 CM-8 NIST 800-53 CM-9 NIST 800-53 PM-5

Last Updated: October, 2018

AM-01 Requirements

1. C&G assets shall adhere to the Information Security requirements defined in these Information Security Standards.

   1.1 Assets may include physical assets, software assets, information assets, data assets, documentation, and services valuable to C&G .

2. Assets must use C&G IT approved operating systems, software and hardware.

3. Information systems within the authorization boundary of an information system must be inventoried as part of that system or recognized by another system as a component within that system.

4. Business/IT owners must ensure there is an authoritative source for inventory which clearly identifies and documents assets within their scope. Existing CMDB and other asset management tools may be used to create and maintain asset inventory.

4.1 Asset inventory must serve as an authoritative source (s) for various security activities across C&G - including but not limited to business critical asset identification, asset criticality assignment, risk assessment, controls implementation, security compliance activities, and other security activities.

4.2 Business Groups may maintain their own asset inventory however; it must serve as an authoritative source for various security activities both, within that Business Group and across C&G .

5. At a minimum, the following information must be documented:

5.1 Asset name

5.2 Asset type

5.3 Asset location details

5.4 Asset description

5.5 Asset ownership

5.6 Asset configurations

5.7 Licensing information

5.8 Change history

5.9 Asset classification (in accordance with C&G information classification scheme)

5.10 Asset status (e.g. Active/Inactive/Disposed)

6. Asset inventory must be reviewed for updates to asset status, asset criticality, and other related information annually at a minimum and/or after a change affecting C&G information systems, infrastructure and/or data. Assets may be reviewed on a more frequent basis, based on applicable business and regulatory requirements.

7. Specific processes must be defined and documented by the business groups for managing end of life product and services. This includes managing the risks of products and services that are no longer available due to suppliers that are no longer in business or suppliers that no longer provide these products and services.

7.1 Systems and products that have reached end-of-life status must be replaced or be decommissioned immediately, where applicable.

7.1.1 In cases where immediate replacement of the system or product is not feasible, the ISO Risk Management team must assign a defined time cap on the usage of outdated models or versions.

7.1.2 Exceptions to the usage of outdated models or versions beyond the time cap must require approval from the head of the respective Business Group and the ISO.

8. Asset inventory must be available for review and audit by C&G according to business needs.

AM-02 Ownership of Assets

C&G assets must have a designated owner.

Owner	Control Mapping

Design Owner: Business/IT Owner Implementation Owner: Business/IT Owner, C&G User	ISO-27002:2013 A.8.1.2	PCI-DSS 12.3.3 PCI-DSS 12.3.4	NIST 800-53 CM-8 NIST 800-53 CM-9 NIST 800-53 PM-5

Last Updated: October, 2018

AM-02 Requirements

1. C&G assets and information must have an assigned ownership to designated C&G IT or business groups.

2. Asset ownership must be assigned when an asset is created or when assets are acquired or transferred to C&G .

3. The asset owner must be accountable for the proper management of an asset over the whole asset lifecycle.

    3.1 Asset owners are accountable for ensuring that assets within their scope are appropriately identified, classified, maintained and updated annually.

    3.2 Asset owners are accountable for ensuring that assets within their scope are appropriately handled and protected across the asset lifecycle in accordance with the defined requirements in these Information Security Standards.

    3.3 Asset owners are accountable for ensuring that their missing or stolen assets are reported immediately, in accordance with the procedures listed on the Corporate Security and Safety page.

4. References and additional requirements related to this control:

    4.1 Media Destruction Standard

AM-03 Acceptable Use

Rules for the acceptable use of information and assets associated with information and information processing facilities must be identified, documented and implemented.

Owner	Control Mapping		
Design Owner: Business/IT Owner Implementation Owner: Business/IT Owner, C&G User	ISO-27002:2013 A.8.1.3 ISO-27002:2013 A.13.2.3	PCI-DSS 12.3.1 PCI-DSS 12.3.5 PCI-DSS 12.3.6 PCI-DSS 12.3.7	NIST 800-53 AC-20 NIST 800-53 PL-4 NIST 800-53 AT-2 NIST 800-53 AC-4 NIST 800-53 SC-05

Last Updated: October, 2018

AM-03 Requirements

1. C&G information systems are intended to be used only for business purposes and in accordance with C&G acceptable use requirements.

2. C&G IT shall maintain a list of approved operating systems and third-party software used by C&G users. This list must be annually reviewed and updated.

2.1 C&G IT must verify the implementation of required security controls as defined in these Information Security Standards on third-party software that process, store or transmit C&G information, in accordance with C&G information security requirements.

3. C&G users must only use third-party software that has been licensed for C&G use and approved by C&G IT. Any installation, distribution or use of any software product that is not licensed for use by C&G is strictly prohibited.

4. Use of external file sharing (P2P, torrent, Dropbox etc.) services on C&G information systems, corporate networks and C&G (both corporate and guest) wireless networks is prohibited.

5. Minimal personal use of C&G photocopy and scanning equipment is allowed.

6. C&G IT shall restrict and periodically monitor for non-C&G approved assets on C&G network for example, unauthorized software, operating system, network scanning devices, hacking tools, mobile devices, proxy servers, anonymous proxy tools, encryption tools, and other unauthorized assets.

7. In the event of unauthorized or inappropriate use of IT assets, appropriate disciplinary action may be taken.

8. C&G users must be made aware of the Information Security requirements related to the usage of C&G assets through training and awareness.

9. C&G business must not be conducted using non-C&G personal email accounts.

9.1 Only C&G domain email addresses are allowed to be member of internal distribution lists.

9.2 Only C&G approved instant messaging services (such as Lync, ICS) must be used to conduct C&G business. External instant messaging services such as instant messaging (e.g. Gmail, Yahoo) must not be used for conducting C&G business or sharing C&G information.

9.3 C&G IT must protect email systems and email messages from denial of service attacks.

9.4 C&G IT must ensure reliability and availability of electronic messaging services.

9.5 C&G users must not use automatic forwarding of electronic mail to external mail addresses for the purposes of conducting C&G business.

9.6 C&G user emails must be backed up and archived by IT.

9.7 Two-factor authentication must be in place to control access to C&G email systems from publicly accessible networks.

10. References and additional requirements related to this control:

10.1 Social Media Policy

10.2 Code of Conduct Policy

10.3 Records Management Policy

10.4 Records Retention Schedule

10.5 OP-06 Information Backup

10.6 HR-04 Disciplinary Process

AM-04 Return of Assets

C&G users must return C&G assets in their possession upon change or termination of their employment, contract or agreement.

Owner	Control Mapping		
Design Owner: Human Resources Implementation Owner: Human Resources, Supervising Manager, IT	ISO-27002:2013 A.8.2.4	PCI-DSS 8.5.4 PCI-DSS 9.2a	NIST 800-53 PS-4 NIST 800-53 PS-5

Last Updated: October, 2018

AM-04 Requirements

1. The HR termination process or change in job role/scope must be formalized to include provisions for the manager to implement the return of previously issued software, corporate documents, and equipment.

    1.1 Other C&G assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media must also be returned.

2. Supervising managers of the terminated C&G user must ensure that assets are returned in accordance with HR termination checklist.

3. In cases where a C&G user purchases C&G equipment or uses their own personal equipment, the supervising manager must ensure that relevant information is transferred back to C&G and is provided to C&G IT for secure disposal.

4. In cases where a C&G user has knowledge that is important to ongoing operations, the manager must ensure that information is documented and transferred to C&G .

5. References and additional requirements related to this control:

    5.1 Termination or Change of Employment

    5.2 HR Termination Checklist (Global + APJ supplemental)

Information Classification

AM-05 Classification of Information

Information must be classified in terms of its business value, legal requirements, sensitivity or criticality to C&G .

Owner	Control Mapping		
Design Owner: ISO Implementation Owner: Business Groups, IT, C&G User	ISO-27002:2013 A.8.2.1	PCI-DSS 9.7.1	NIST 800-53 RA-2

Last Updated: October, 2018

AM-05 Requirements

1. C&G users are required to classify information (both physical and electronic) as highly confidential, confidential, private or public to protect the confidentiality, integrity and availability of C&G assets, information and technology resources in accordance with C&G information classification scheme.

2. Assets other than information must be handled in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

3. Appropriate level of security controls shall be implemented for different information classes based on the information classification scheme and security requirements defined in these Information Security Standards and C&G information classification scheme.

4. Asset owners must appropriately classify and protect and regularly review and update information within their assets.

5. Information shall be considered "Confidential" by default. Information that has not been classified is to be treated as “Confidential” until a determination is made that the information is either

   5.1 Not “C&G Internal - Confidential” (or lower) and therefore could be released publicly, or to business prospects, without limitation, or

   5.2 “C&G Internal - Confidential” (or higher) and therefore must have greater restrictions on handling/dissemination.

6. C&G highly confidential and confidential information shall only be disclosed outside C&G to companies and individuals who have properly executed a Non-Disclosure / Confidentiality Agreement or regulatory requirement.

7. References and additional requirements related to this control:

   7.1 Information Classification and Handling Standard

AM-06 Labeling of Information

An appropriate set of procedures for information labeling must be developed and implemented in accordance with the information classification scheme adopted by C&G .

Owner	Control Mapping		
Design Owner: ISO Implementation Owner: Business Groups, IT, C&G User	ISO-27002:2013 A.8.2.2	PCI-DSS 12.3.4	NIST 800-53 MP-2 NIST 800-53 MP-3

Last Updated: October, 2018

AM-06 Requirements

1. C&G assets, information and technology resources (both physical and electronic) shall be labeled and handled in accordance with C&G information classification scheme.

2. Assets, information and technology resources that are not labeled (due to business exceptions) must be appropriately controlled and protected through compensating controls by the respective asset owners.

3. References and additional requirements related to this control:

   3.1 Information Classification and Handling Standard

AM-07 Handling of Assets

Procedures for handling assets must be developed and implemented in accordance with the information classification scheme adopted by C&G .

Owner	Control Mapping		
Design Owner: ISO Implementation Owner: Business Groups, IT, C&G User	ISO-27002:2013 A.8.2.3	PCI-DSS 9.6 PCI-DSS 9.7 PCI-DSS 9.8 PCI-DSS 9.9	NIST 800-53 MP- Family NIST 800-53 SI-12

Last Updated: October, 2018

AM-07 Requirements

1. The handling, processing, storage, and communication of C&G information must be consistent with C&G information classification scheme.

2. The following procedures shall be defined, documented and implemented by the information asset owner, wherever applicable:

   2.1 Handling and labeling of media shall be performed in accordance with the classification level of the information contained in the media.

   2.2 Distribution of data must be limited on a “need-to-know” basis only and distribution lists reviewed at regular intervals.

   2.3 Logical and physical access restrictions, as applicable, must be implemented to prevent access to unauthorized personnel.

   2.4 Media storage shall be in accordance with manufacturers' specifications and C&G Information Security Standards.

   2.5 Copies of media must be clearly marked for the attention of the authorized recipient.

3. Agreements with other organizations that include information sharing must include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

4. References and additional requirements related to this control:

   4.1 Information Classification and Handling Standard

Media Handling

AM-08 Management of Removable Media

Procedures must be implemented for the management of removable media in accordance with the classification scheme adopted by C&G .

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT, C&G User	ISO-27002:2013 A.8.3.1	PCI-DSS 3.4.1 PCI-DSS 9.6 PCI-DSS 12.3.10	NIST 800-53 AC-19 (2) NIST 800-53 AC-19 (3) NIST 800-53 MP-Family

Last Updated: October, 2018

AM-08 Requirements

1. Only C&G -IT approved removable media and storage devices must be used to store C&G information.

   1.1 If no longer required, the contents of any re-usable media that are to be removed from C&G must be made unrecoverable.

   1.2 Where necessary and practical, authorization from the respective system/asset owner should be required for media removed from C&G information processing facilities and a record of such removals shall be kept in order to maintain an audit trail.

   1.3 Media must be stored in a safe, secure environment, in accordance with manufacturers' specifications.

2. Information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers' specifications) must be replicated elsewhere to avoid information loss due to media deterioration.

3. Usage of personal removable media drives is strictly prohibited.

4. Procedures and access rights for the usage of removable media shall be clearly documented.

5. References and additional requirements related to this control:

   5.1 Records Management Policy

   5.2 Records Retention Schedule

   5.3 Media Destruction Standard

AM-09 Disposal of Media

Media must be disposed of securely when no longer required, using formal procedures.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT, C&G User	ISO-27002:2013 A.8.3.2	PCI-DSS 3.1 PCI-DSS 9.10	NIST 800-53 MP-4 NIST 800-53 MP-6

Last Updated: October, 2018

AM-09 Requirements

1. C&G data storage mediums must follow C&G approved media destruction mechanisms for secure and safe disposal/destruction of media.

   1.1 External third-party storage providers (such as cloud storage providers) must use C&G equivalent media destruction mechanisms for secure and safe disposal/destruction of C&G media.

2. Media destruction procedures for secure disposal of media containing non-public information must be commensurate with the criticality of that information.

   2.1 Approved third-party services to perform data destruction services must be used.

3. References and additional requirements related to this control:

    3.1 Media Destruction Standard

AM-10 Physical Media Transfer

Media containing information must be protected against unauthorized access, misuse or corruption during transportation.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 8.3.3	PCI-DSS 9.5.a PCI-DSS 9.6 PCI-DSS 9.7.2	NIST 800-53 MP-5

Last Updated: October, 2018

AM-10 Requirements

1. Based on the business and regulatory requirements, physical media in transfer should be encrypted.

2. There shall be documented procedures for the identification of courier service provider.

3. C&G -approved transport or couriers must be used for transfer of media, in accordance with C&G information classification scheme.

4. Media packaging must ensure that the content is protected from any environmental damage likely to arise during transit and in accordance with media manufacturer's specifications.

5. Logs of media transport must include:

    5.1 Identification for the media

    5.2 The information security controls (encryption, secure packaging, etc.) applied to the media

    5.3 Times of transfer to the transit custodians

    5.4 Times of receipt at the destination

This page is intentionally left blank.

Information Security Standard Four: Logical Access Control Security Standard

Information Security Standard Objective	
This Information Security Standard is established to control logical access (both privileged and non-privileged) to information, networks and C&G assets.	
Control Categories	**Controls**
Business requirements of logical access control *To limit logical access to information and information processing facilities.*	• AC-01 Logical Access Control Policy, Standards and Procedures • AC-02 Logical Access to Network and Network Services
Logical access management *To ensure authorized user access and to prevent unauthorized logical access to systems and services.*	• AC-03 User Registration and De-registration • AC-04 Logical Access Authorization • AC-05 Management of Privileged Access Rights • AC-06 Management and Use of Secret Authentication Information of Users • AC-07 Review of User Access Rights • AC-08 Removal or Adjustment of Access Rights • AC-09 Logical Authentication Procedures

Business Requirements of Logical Access Control

AC-01 Logical Access Control Policy, Standards and Procedures

Logical access to C&G information assets shall only be provided based on legitimate and authorized business needs, using the concept of least privileges.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.1.1 ISO-27002:2013 A.9.4.1 ISO-27002:2013 A.9.4.5	PCI-DSS 7 PCI-DSS 9 PCI-DSS 8.5.16	NIST 800-53 AC-1 NIST 800-53 AC-2 NIST 800-53 AC-3 NIST 800-53 AC-6 (1) NIST 800-53 AC-21 NIST 800-53 PE-1 NIST 800-53 PE-2 NIST 800-53 SA-10

Last Updated: October, 2018

AC-01 Requirements

1. Access to C&G information shall only be provided based on legitimate and authorized business needs and using the concept of least privileges (default deny all setting).

   1.1 Access rights to systems and applications for users (e.g. ability to perform read, write, update or delete operations) must be restricted.

2. Asset owners are accountable for controlling logical access to their information systems and information assets.

3. Asset owners are accountable for establishing and documenting access procedures for their information systems and assets.

4. Authentication to information systems, facilities and information assets must be in accordance with the following requirements:

Information Classification Type	Authentication Type
Ability to access/modify Highly Confidential Information	Strong Authentication (two or more forms of authentication)
Ability to access/modify Confidential Information	Single Factor Authentication
Ability to access/modify Private Information	Single Factor Authentication
Public Information	Optional

5. Outputs from systems and applications handling highly confidential or confidential information must contain only the information relevant to the use of the output.

6. Based on the business needs, logical information security controls should be in place for the isolation of applications, systems or assets.

7. For physical access requirements, refer to:

   7.1 Secure Areas

AC-02 Logical Access to Network and Network Services

Logical access to the network and network services shall only be provided based on legitimate and authorized business needs, using the concept of least privileges.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.1.2 ISO-27002:2013 A.9.4.4	PCI-DSS 7 PCI-DSS 1.1.4	NIST 800-53 AC-1 NIST 800-53 AC-5 NIST 800-53 AC-6(3) NIST 800-53 AC-17 NIST 800-53 AC-18 NIST 800-53 AC-20 NIST 800-53 MA-2 NIST 800-53 MA-3 NIST 800-53 MA-4

Last Updated: October, 2018

AC-02 Requirements

1. Only C&G IT approved network infrastructure devices shall be used on C&G networks. Examples of network infrastructure devices include routers, switches, wireless access points, portable Wi-Fi devices, hotspots etc.

   1.1 Usage of non-C&G owned network infrastructure devices on C&G networks for business purposes (e.g. testing in engineering labs) must be explicitly approved by the heads of the respective Business Groups, C&G IT and the ISO.

   1.2 Use of network infrastructure devices (tethered smartphone, MiFi etc.) for Internet access or remote connection to C&G network (through C&G VPN) is allowed.

2. Use of network services handling highly confidential or confidential information must be logged and monitored on a regular basis.

3. Only C&G IT issued and approved WAP hardware must be deployed on C&G networks.

4. Information systems connected to C&G corporate network or C&G internal wireless infrastructure must be authenticated.

   4.1 Non-C&G approved devices are not allowed to connect to C&G corporate network or C&G internal wireless infrastructure.

5. Guest wireless network for Internet-only access shall be provided to visitors and external parties at C&G locations.

   5.1 Guest wireless networks must be clearly separated from C&G corporate network and C&G internal wireless infrastructure.

   5.2 Only registered visitors shall be allowed access to guest wireless networks for a defined period of time.

   5.3 A bandwidth usage limit must be in place for everyone that uses these guest wireless networks.

   5.4 Visitors are ultimately responsible for the security of their devices.

   5.5 Unauthorized or inappropriate use of guest wireless networks is prohibited.

   5.6 Guest connecting to C&G wireless network must be subject to DLP monitoring and must be issued a warning to protect C&G information assets in accordance with C&G information security requirements.

6. The use of privileged utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled. Examples of privileged utility programs include anti-virus software, backup software, patch management software, vulnerability scanning software, network utilities, system monitoring software, disk management software etc.

   6.1 Utilities must be segregated from the applications software.

   6.2 There shall be a limitation on the use of privileged utilities to a minimum number of authorized administrators only.

   6.3 The availability of system utilities to execute privileged commands shall be restricted to a limited period of time.

   6.4 Use of system utilities must be logged and monitored.

   6.5 Authorization levels for system utilities must be defined and documented.

   6.6 Unnecessary utilities and system software must be removed or disabled.

7. References and additional requirements related to this control:

   7.1 Network Access Standard

   7.2 Security Zone Standard

   7.3 Logging and Monitoring

7.4 Wireless Access Point Standard

7.5 AM-03 Acceptable Use

7.6 Remote Access Standard

7.7 Bastion Host Standard

7.8 Risk Acceptance Process

Logical Access Management

AC-03 User Registration and De-Registration

A formal user (both individual and service accounts) registration and de-registration procedure must be implemented for granting and revoking logical access for all user types to all systems and services.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.2.1	PCI-DSS 8.1 PCI-DSS 8.5 PCI-DSS 8.5.8	NIST 800-53 AC-1 NIST 800-53 AC-2

Last Updated: October, 2018

AC-03 Requirements

1. Domain accounts and email address that are issued by C&G shall be unique for up to 30 days after termination and must not be shared by other users.

    1.1 Use of shared IDs or accounts must only be performed for business and operational reasons with a documented approval from the heads of the respective Business Groups. Other compensating controls must be used if shared IDs or accounts are used.

    1.2 Misrepresenting, obscuring, suppressing, or changing user identities are strictly prohibited.

    1.3 User name, email address, C&G affiliation, and related information included in messages or files shall clearly identify the actual originator of those message or files.

    1.4 Account username and password must not be written down, shared or distributed to other users.

2. User IDs and credentials for terminated users shall be immediately disabled or removed.

3. Inactive user IDs and accounts shall be reviewed every 90 days and shall be removed or blocked.

AC-04 Logical Access Authorization

A formal user access authorization process must be implemented to assign or revoke access rights for all user types to all information systems and assets.

Owner	Control Mapping		
Design Owner: IT, Business Groups	ISO-27002:2013 A.9.2.2	PCI-DSS 7.1.4 PCI-DSS 8.5.4	NIST 800-53 AC-2 NIST 800-53 IA-2 NIST 800-53 IA-5

Implementation Owner: Business Groups, IT			

Last Updated: October, 2018

AC-04 Requirements

1. C&G users shall receive authorization for the use of information systems and assets from the respective system or service owner.

2. C&G users must not be provided access until authorization procedures have been completed.

3. Business/IT owner shall maintain a formal record (user access requests/approvals etc.) of all users registered to use information systems that hold highly confidential information.

4. Business/IT owner shall immediately remove or block access rights of users who have been terminated or have changed roles within C&G .

5. The level of access granted shall be verified to ensure that it is appropriate to the business purpose and is consistent with C&G Information Security Policy (e.g. not compromising segregation of duties).

6. An identity and access management system shall be implemented for access authorization of systems storing highly confidential information.

AC-05 Management of Privileged Access Rights

The allocation and use of privileged access rights must be restricted and controlled.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.2.3	PCI-DSS 7.1.1 PCI-DSS 7.1.2 PCI-DSS 7.1.3 PCI-DSS 7.2.2	NIST 800-53 AC-6(2)

Last Updated: October, 2018

AC-05 Requirements

1. A formal and documented authorization process shall be established for determining access privileges associated with information systems, facilities and information assets.

2. Privileged access rights for information systems must be provided on a “need to know” basis using the concept of least privilege for a defined period of time.

    2.1 Business/IT owners shall identify and document the expiry period for privileged access rights granted to C&G users.

3. Based upon the formal authorization process that is established, a record of all privileged access rights allocated shall be maintained.

4. Changes to privileged access rights must be documented and require explicit and documented approval from the respective Business/IT owners.

5. Regular business activities must not be performed from privileged accounts. Privileged access rights must be assigned to a user ID different from those used for regular business activities.

6. Unused generic administration accounts (e.g. domain accounts, vendor accounts, shared accounts, anonymous FTP) must be disabled.

7. Unauthorized use of generic administration accounts (e.g. domain accounts, vendor accounts, shared accounts, anonymous FTP) must be prohibited.

8. References and additional requirements related to this control:

   8.1 Records Management Policy

   8.2 Records Retention Schedule

AC-06 Management and Use of Secret Authentication Information

The use of secret authentication information must be controlled through a formal management process.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.2.4 ISO-27002:2013 A.9.3.1 ISO-27002:2013 A.9.4.3	PCI-DSS 8.4 PCI-DSS 8.5.2 PCI-DSS 8.5.3 PCI-DSS 8.5.7 PCI-DSS 8.5.9 PCI-DSS 8.5.10 PCI-DSS 8.5.11 PCI-DSS 8.5.12 PCI-DSS 8.5.13 PCI-DSS 8.5.14	NIST 800-53 IA-2 NIST 800-53 IA-5 (1)

Last Updated: October, 2018

AC-06 Requirements

1. C&G users shall receive initial, replacement or temporary authentication information via a secure method. Some viable options are -

   1.1 Telephone – The authentication information itself may be revealed over the phone upon positively validating the individual's identity.

   1.2 Email – The user ID or authentication information can be sent to the user via signed and encrypted corporate email (C&G .com) or via C&G -approved and managed corporate mobile devices such as laptops, smartphones, tablet computers, etc. The use of any other medium is prohibited. The email must not be permitted to be copied (cc'd) to anyone else.

2. Leaving authentication information via voicemail message or via unprotected clear text is prohibited.

3. Users shall be required to change their temporary authentication information upon first logon.

4. C&G users shall immediately change authentication information or obtain new authentication information whenever there is any indication of its possible compromise.

5. C&G users shall never share their authentication information or other identity information (access badges, secret keys etc.) with anyone.

6. C&G users must not use their same authentication information for business and non-business purposes.

7. Temporary authentication information shall be unique to each user. Temporary authentication information shall follow the C&G standard authentication information and transmission requirements (length, complexity, lockout, etc.).

8. Password initialization or reset must validate a user's identity using established "pre-shared information" before securely transferring the password to the individual. The pre-shared information may be either a shared secret or a secured identifier (e.g. C&G user ID) associated with the user.

9. Users shall acknowledge the receipt of authentication information.

10. Authentication information shall never be stored on computer systems in an unprotected form.

    10.1 Passwords must be stored using one-way encryption techniques (i.e., a password cannot be decrypted into clear text).

    10.2 Passwords must not be stored in readable form in batch files, command files, automatic login scripts, shell scripts, communication scripts, software macros, terminal function keys, in systems without access control, or in other locations where unauthorized persons might discover them.

    10.3 Password files must be stored separately from application system data.

11. Default authentication information within software products and hardware must be changed prior to or during installation.

12. Authentication information is classified as highly confidential information and shall be protected in accordance with C&G information classification scheme.

13. Information systems and assets shall use complex authentication requirements considering the criticality of information stored inside those information systems. The minimum requirements for password complexity include:

    13.1 Must not be the same as the username / user ID.

    13.2 Must not contain a word found in the dictionary.

    13.3 Must contain at least one number or other non-alphabetic character.

    13.4 Must use both upper and lower case letters.

    13.5 Must be a minimum of eight characters long.

    13.6 Reuse of at least the previous 6 passwords is not allowed.

    13.7 Must be unique and difficult to guess.

14. Authentication information must expire every 90 days and must not be changeable within 1 day of the previous change, except in the case where the authentication information has been compromised.

15. The maximum number of times a password can be attempted is 5 within 15 minutes.

    15.1 A warning message must be sent to the system administrator after the maximum number of failed logon attempts has been reached.

    15.2 After the threshold is met, the user account must be suspended or disabled.

    15.3 Account lockouts must be a minimum of 60 minutes, unless unlocked by an administrator.

15.4 Only authorized C&G IT administrators shall be allowed to activate suspended or disabled accounts.

16. The method of storage of authentication information (e.g. passwords, secret codes) must be C&G -approved.

17. Password management systems shall be used to validate the password construction and complexity. These systems must not compromise the passwords.

18. Password management systems must enforce the use of individual user IDs and passwords to maintain accountability.

19. Password management systems must allow users to select and change their own passwords via self-service and provide confirmation procedures to allow for input errors.

    19.1 Password management systems may be configured to allow users to answer self-configured security questions prior to resetting their passwords.

    19.2 Additional security controls for password self-service such as verification code sent by SMS may be used for information systems storing highly confidential information.

20. Password management systems must enforce change of password after first logon.

21. Password management systems must maintain the records of any password changes.

22. Passwords must not be displayed while authenticating to information systems.

23. References and additional requirements related to this control:

    23.1 Logging and Monitoring

AC-07 Review of User Access Rights

Business groups must review users' access rights at regular intervals.

Owner	Control Mapping		
Design Owner: Business Groups Implementation Owner: Business Groups	ISO-27002:2013 A.9.2.5	PCI-DSS 8.5.4 PCI-DSS 8.5.5 PCI-DSS 8.5.6	NIST 800-53 AC-2 NIST 800-53 PE-2

Last Updated: October, 2018

AC-07 Requirements

1. System owners shall review user access rights to monitor any changes such as promotion, transfer, demotion or termination of employment.

    1.1 Access rights for highly confidential or confidential information must be reviewed every 60 days.

    1.2 Access rights for all other information shall be reviewed every 90 days to ensure that unauthorized privileges have not been obtained.

2. Changes to special privileged accounts must be logged for periodic review.

3. Review of remote access activities shall be in accordance with any regional or national regulatory requirements.

4. References and additional requirements related to this control:

   4.1 Remote Access Standard

AC-08 Removal or Adjustment of Access Rights

The access rights of C&G users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Owner	Control Mapping		
Design Owner: Business Groups Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.2.6	PCI-DSS 8.5.4	NIST 800-53 IA-2 NIST 800-53 IA-5

Last Updated: October, 2018

AC-08 Requirements

1. Upon termination, the access rights of an individual to information and assets associated with information processing systems and facilities must be removed or suspended within 24 hours of notification.

2. Changes of employment must be reflected in removal of access rights that were not approved for the new employment.

   2.1 Supervising manager must notify Human Resources for any such changes to ensure that physical and logical access rights are re-allocated accordingly.

3. Any documentation that identifies access rights of C&G users must reflect the removal or adjustment of access rights.

4. If a departing C&G user knows any active passwords for shared or service accounts, they must be changed upon termination or change of employment, contract or agreement.

   4.1 In circumstances where the departing C&G user was using a group or shared account, he shall be removed from the group access list and an email notification must be sent to other members of the group by the system owner to no longer share this information with the departing user. Password or access credentials should be changed immediately, where applicable.

AC-09 Logical Authentication Procedures

Access to information systems and applications must be controlled by logical authentication procedures, based on the information classification scheme.

Owner	Control Mapping		
Design Owner: Business Groups, IT Implementation Owner: Business Groups, IT	ISO-27002:2013 A.9.4.2	PCI-DSS 8.2 PCI-DSS 8.3 PCI-DSS 8.5.15	NIST 800-53 AC-7 NIST 800-53 IA-5 NIST 800-53 IA-5(1) NIST 800-53 IA-6

Last Updated: October, 2018

AC-09 Requirements

1. Suitable authentication mechanisms shall be used to substantiate the claimed identity of a user.

2. When strong authentication is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens, biometrics etc. must be used.

   2.1 Two-factor authentication for remote access must be implemented for access to C&G corporate network.

3. The log-on procedure for an information system must disclose minimum information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

   3.1 The information system or application must not display identifiers until the log-on process has been successfully completed.

   3.2 The information system or application shall display a general notice warning that the computer shall only be accessed by authorized users.

   3.3 Help messages must not be provided during log-on procedures that would possibly aid an unauthorized user.

   3.4 Log-on information shall be validated only upon completion of all input data.

      3.4.1 Upon failed authentication, the system must not indicate which part of the credential is correct or incorrect.

4. The information system or application must be protected against brute force logon attempts.

5. The information system or application shall terminate inactive sessions after a defined period of time, especially from remote devices accessing C&G network from remote locations.

   5.1 The information system or application shall terminate active sessions associated with authenticated user if those credentials are used to initiate a new session, to avoid concurrent sessions.

6. For cardholder data, if the session has been idle for 15 minutes, user shall be required to re-authenticate to reactivate the session.

7. The following information may be displayed upon completion of a successful log-on:

   7.1 Date and time of the previous successful log-on.

   7.2 Details of any unsuccessful log-on attempts since the last successful log-on.

8. References and additional requirements related to this control:

   8.1 Remote Access Standard

This page is intentionally left blank.

Information Security Standard Five: Cryptography Security Standard

Information Security Standard Objective	
This Information Security Standard is established to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of C&G information.	
Control Categories	**Controls**
Cryptographic Controls *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.*	• CM-01 Use of Cryptographic Controls • CM-02 Key Management

Cryptographic Controls

CM-01 Use of Cryptographic Controls

Cryptographic controls for protection of C&G information must be developed, implemented and reviewed on a periodic basis.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.10.1.1	PCI-DSS 8.4 PCI-DSS 2.3 PCI-DSS 4.1 PCI-DSS 4.1.1	NIST 800-53 IA-7 NIST 800-53 SC-8(1) NIST 800-53 SC-9 NIST 800-53 SC-13

Last Updated: October, 2018

CM-01 Requirements

1. Cryptography at C&G should be used to provide confidentiality, integrity, and authenticity of data.

   1.1 Based on the business needs, business risks and C&G information classification scheme; the required level of encryption must be identified and implemented by the Business/IT owner in consultation with the ISO taking into account the type, strength, and quality of the cryptographic algorithm required.

2. ISO-approved cryptographic controls must be used for the protection of highly confidential stored, processed or transmitted data by information systems, mobile or removable media, devices, C&G networks, wireless access points, over the Internet, over mobile networks (GSM, GPRS etc.) or across communication lines.

   2.1 Some examples include use of database-level encryption for storage of data, use of cryptography (e.g. SSL/HTTPS) for highly confidential information transmitted over public networks, etc.

3. Cryptographic controls may be used for other information classification types, depending on the business needs and risk to C&G .

4. For information systems in-scope of PCI-DSS, non-console administrative access must be encrypted using strong cryptographic mechanisms such as use of SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

5. Tokenization may be used – alternatively or in addition to cryptography - as a means for protecting highly confidential information in order to comply with Information Security regulations and standards.

6. Usage of weak security encryption algorithms (e.g. WEP/WPA1 for wireless devices), weak algorithm modes or weak key sizes identified by the ISO is not allowed.

7. Wireless networks must implement strong cryptographic mechanisms based on ISO-approved mechanisms for authentication and transmission.

8. Cryptography procedures shall be defined and documented including:

    8.1 Instructions for the implementation of cryptographic controls.

    8.2 Instructions for key management, including key generation, key expiry and rollover of keys.

    8.3 Instructions for the usage of specific cryptographic mechanisms with their functionality and limitations.

    8.4 The impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).

    8.5 Roles and responsibilities of entities implementing cryptography.

9. The use of cryptography must comply with applicable local and national government regulations and export control requirements and must consider issues of trans-border flow of encrypted information.

10. Authentication information (i.e. passwords) must be protected during transmission and storage using strong cryptography.

11. Information systems must run a C&G IT approved and managed encryption solution (such as disk/email encryption) to ensure the security and confidentiality of C&G information. The encryption solution must ensure that:

    11.1 Encryption methods used are approved by the ISO.

    11.2 Central key management process is implemented by C&G IT on supported platforms.

    11.3 Events are logged and monitored.

12. References and additional requirements related to this control:

    12.1 Wireless Access Point Standard

    12.2 Logging and Monitoring

    12.3 Database Encryption Key Management Standard

    12.4 Cryptography Review Board Page

CM-02 Key Management

Information Security controls for the use, protection, rollover, and lifetime of cryptographic keys must be developed, implemented and reviewed on a periodic basis throughout their whole lifecycle.

Owner	Control Mapping		
Design Owner: ISO, Business Groups	ISO-27002:2013 A.10.1.2	PCI-DSS 3.5 PCI-DSS 3.6	NIST 800-53 SC-12 NIST 800-53 SC-17

Implementation Owner: IT, Business Groups			

Last Updated: October, 2018

CM-02 Requirements

1. Cryptographic keys must be classified as highly confidential information.

    1.1 Appropriate Information Security controls shall be implemented for the protection of cryptographic keys, in accordance with C&G information classification scheme.

2. Equipment used to generate, store and archive cryptographic keys must be physically protected (e.g. through data center access controls, securing storage locations, and other physical security controls.

3. Cryptographic keys must be protected against modification, loss, and destruction.

    3.1 Secret and private keys must be protected against unauthorized disclosure.

4. Cryptographic key management systems must have defined and documented procedures for the following areas:

    4.1 Generating cryptographic keys for different cryptographic systems and different applications.

    4.2 Generating and obtaining public cryptographic key certificates.

    4.3 Distributing cryptographic keys to intended users, including how keys should be activated when received.

    4.4 Storing cryptographic keys, including how authorized users obtain access to keys.

    4.5 Changing or updating cryptographic keys including rules on when keys must be changed.

    4.6 Handling compromised cryptographic keys.

    4.7 Activating, deactivating, and revoking cryptographic keys.

        4.7.1 Activation and deactivation dates for cryptographic keys must be defined to ensure that keys can only be used for a limited period of time.

        4.7.2 Activation and deactivation period of cryptographic keys must be dependent on the business needs and risk to C&G .

    4.8 Recovering cryptographic keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information.

    4.9 Archiving cryptographic keys, e.g. for information archived or backed up.

    4.10 Data retention policy for cryptographic keys.

    4.11 Destroying cryptographic keys.

5. Logging and monitoring of key management activities must be performed at defined intervals, depending on the business needs.

6. Cryptographic keys used for encryption must be rotated at defined intervals. The key rotation process must remove an old key from the encryption/decryption process and replace it with a new key.

7. In the event the integrity of a key is weakened or a key is suspected of compromise, the key must be replaced or retired.

   7.1 If the retired or replaced cryptographic key needs to be retained, the key must be securely archived.

8. The authenticity of public cryptographic keys must be defined and controlled. This authentication process can be done using public key certificates that are normally issued by a certification authority.

   8.1 The certification authority must be a recognized organization – preferably C&G Trust Services - with suitable controls and procedures in place to provide the required degree of trust.

9. Access to cryptographic keys must be restricted on a need-to-know basis.

10. Cryptographic keys must be securely stored and controlled.

11. If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).

12. Unauthorized substitution of cryptographic keys must be prevented.

13. Key custodians shall formally acknowledge that they understand and accept their key-custodian responsibilities using the Key Custodian Acknowledgement Form.

14. References and additional requirements related to this control:

   14.1 Secure Areas

   14.2 Equipment

   14.3 Records Management Policy

   14.4 Records Retention Schedule

   14.5 Security in Supplier Relationships

   14.6 Logging and Monitoring

   14.7 Media Destruction Standard

   14.8 OP-06 Information Backup

   14.9 Database Encryption Key Management Standard

This page is intentionally left blank.

Information Security Standard Six: Physical and Environmental Security Standard

Information Security Standard Objective	
This Information Security Standard is established to prevent unauthorized physical access, damage, and interference to C&G premises and information.	
Control Categories	**Controls**
Secure Areas *To prevent unauthorized physical access, damage and interference to C&G information and information processing facilities*	• PE-01 Physical Security Perimeter • PE-02 Physical Entry Controls • PE-03 Securing Offices and Rooms • PE-04 Protecting against External and Environmental Threats • PE-05 Securing Restricted Access Areas • PE-06 Delivery and Loading Areas
Equipment *To prevent loss, damage, theft or compromise of assets and interruption to C&G operations.*	• PE-07 Equipment Siting and Protection • PE-08 Supporting Utilities • PE-09 Cabling Security • PE-10 Equipment Maintenance • PE-11 Removal of Assets • PE-12 Physical Security of Equipment and Assets Off-premises • PE-13 Secure Disposal or Reuse of Equipment • PE-14 Unattended User Equipment (e.g. information system, workstation, laptop, smartphone) • PE-15 Clear Desk and Clear Screen Requirements

Secure Areas

PE-01 Physical Security Perimeter

Physical security perimeters must be defined and used to protect information processing facilities, based on the business needs, criticality of information housed and risks to C&G .

Owner	**Control Mapping**		
Design Owner: Business Groups Implementation Owner: GFM	ISO-27001:2013 A.11.1.1	PCI-DSS 9.1	NIST 800-53 PE-3

Last Updated: October, 2018

PE-01 Requirements

1. Perimeters of C&G locations such as data centers, storage locations, and general office space shall be physically secured. The level of physical security controls required for a particular location shall be based on the business needs, criticality of information housed and risks to C&G .

2. External walls of the site shall be of solid construction.

3. Doors and windows shall be locked when unattended, allowing only authorized personnel to access the location.

3.1 Accessible doors and operable windows on the perimeter shall have additional external protections such as an alarm system.

3.2 External doors that are not used as common access/entry points shall be locked and alarmed at all times. Alarms must be reported to and responded by Corporate Security and Safety.

3.3 External doors that are used as common access/entry points shall be alarmed as required; however, at a minimum, they shall be alarmed outside of normal business hours.

3.4 Fire doors on a security perimeter shall be alarmed, monitored, and tested in conjunction with the walls in accordance with the certifying or authority having jurisdiction to establish the required level of fire resistance in accordance with local fire code.

4. External lighting shall be of sufficient brightness and positioned in a way that enhances the security and safety of C&G premises.

5. External lighting must not be positioned in such a way that will impact an individual’s night vision when looking away from the building or site, toward the perimeter.

6. Physical barriers shall, where applicable, be built to prevent unauthorized physical access and environmental contamination.

7. The applicability of physical barriers shall be determined based on the business needs and risks to C&G information.

8. Shrubbery, trees and/or pertinent structures should be placed and/or maintained in such a manner as not to allow for the concealment of potential intruders, or for the opportunity to bypass security safeguards.

9. Intrusion alarm systems shall be installed to meet applicable national, regional, or international standards and must be tested regularly.

10. Where provided, intrusion alarm systems shall be turned on during times when the space is not in use.

11. Data centers, call centers, offices and other facilities managed by C&G should be physically separated from those managed by third parties.

    11.1 In cases where it has been determined by the respective head of the Business Group and the ISO that a particular facility such as data center/enhanced eSuites must be shared with a third party, all C&G -owned and managed IT assets, supporting software and documentation shall be housed securely in a network rack, safe, file cabinet, etc. managed by the respective Business Groups and separated from other third parties.

12. C&G information processing facilities and users must adhere to the general physical and environmental security requirements defined by the Corporate Security and Safety and Facilities.

PE-02 Physical Entry Controls

C&G facilities must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Owner	Control Mapping		
Design Owner: GFM, Business Groups Implementation Owner: Corporate Security and Safety, Business Groups	ISO-27001:2013 A.11.1.2	PCI-DSS 9.1 PCI-DSS 9.1.1 PCI-DSS 9.2 PCI-DSS 9.3 PCI-DSS 9.4	NIST 800-53 PE-2 NIST 800-53 PE-3 NIST 800-53 PE-7 NIST 800-53 PE-8

Last Updated: October, 2018

PE-02 Requirements

1. C&G facilities must have a formal method of controlling access. Business groups shall provide a method for identifying all persons authorized to access a C&G -managed facility, along with a method for controlling access.

   1.1 Physical access to C&G facility must be based on legitimate and authorized business needs.

      1.1.1 Physical access to restricted access areas shall be restricted to authorized C&G users only.

   1.2 Physical access rights must be reviewed on a half-yearly basis and/or based on the business needs and perceived risks to the information facility such as data center, offices, engineering labs and storage locations.

   1.3 Audit trail of physical access to restricted access areas shall be maintained and stored for a minimum of 90 days.

   1.4 Access to restricted access areas shall be tightly controlled and approved by a Restricted Access Area Manager or appropriately escorted by authorized personnel.

2. Access to the badge granting system must be controlled on a need-to-know basis only.

3. The following processes and procedures shall be in-place for assigning badges to users and visitors:

   3.1 Granting new and temporary badges.

   3.2 Changing access requirements.

   3.3 Revoking access privilege as necessary.

4. C&G users that require access to a C&G location shall be issued a C&G photo ID access badge.

5. C&G photo ID access badges shall be re-issued upon loss of badge, name change, or critical change of a person’s appearance.

   5.1 C&G photo ID access badges remain the property of C&G and shall be returned to management, upon request.

   5.2 C&G photo ID access badges shall be clearly displayed at all times.

   5.3 C&G users shall take appropriate action if they encounter unescorted visitors or anyone not wearing a visible C&G Photo ID Access Badge.

   5.4 When a C&G user determines that his/her C&G -issued ID badge has been lost or misplaced, Corporate Security and Safety must be notified immediately for deactivation.

6. Visitors shall be escorted and supervised.

7. Visitors shall be issued a visitor badge.

   7.1 A record/log of all visitors (including third-party support service personnel), shall be kept in order to maintain a physical audit trail of visitor activity. At a minimum, the visitor log shall record the following information: Date of Visit; Name; Company; C&G Point of Contact; Arrival Time; Departure Time.

7.2 Visitor log shall be retained in accordance with the records retention policy.

7.3 Visitors leaving the facility shall be asked to surrender visitor badge upon departure or expiration.

8. Temporary access ID badges shall be uniquely numbered, controlled, and inventoried at the beginning and end of each business day.

8.1 Temporary access ID badges to physical areas that store cardholder data shall be controlled by the business groups to verify that a badge does not permit unescorted access, unless such access has been formally approved.

8.2 Temporary access ID badges can be issued to C&G users who have forgotten their badges for a day, after appropriate identity verification. With issuance of this temporary access badge, C&G users may be granted access to areas previously-approved with the temporary ID badge.

PE-03 Securing Offices and Rooms

Physical security for offices and rooms must be designed and implemented.

Owner	Control Mapping		
Design Owner: GFM Implementation Owner: GFM, CSS, Business Groups	ISO-27001:2013 A.11.1.3	PCI-DSS 9.1.2 PCI-DSS 9.1.3	NIST 800-53 PE-3 NIST 800-53 PE-5 NIST 800-53 PE-6(1) NIST 800-53 PE-7 NIST 800-53 PE-16 NIST 800-53 PE-18

Last Updated: October, 2018

PE-03 Requirements

1. Offices, rooms, and other facilities shall be secured in such a manner as not to conflict with or violate local, state, national, or international health and safety regulations and standards.

2. System logs shall record physical access and be retained consistent with the records retention policy.

PE-04 Protecting Against External and Environmental Threats

Physical protection against external and environmental threats such as natural disasters, malicious attacks or accidents must be designed and applied.

Owner	Control Mapping		
Design Owner: Corporate Security and Safety, GFM Implementation Owner: Corporate Security and Safety, GFM	ISO-27001:2013 A.11.1.4	PCI-DSS 9.9	NIST 800-53 CP-1 NIST 800-53 CP-2 NIST 800-53 CP-6 NIST 800-53 CP-7 NIST 800-53 CP-7(1) NIST 800-53 PE-1 NIST 800-53 PE-9 NIST 800-53 PE-10 NIST 800-53 PE-11 NIST 800-53 PE-13 NIST 800-53 PE-15

Last Updated: October, 2018

PE-04 Requirements

1. Hazardous or combustible materials shall be stored at a safe distance from secure areas and in accordance with local, state, and national laws and regulations.

2. Backup equipment and media shall be sited at a reasonable distance from the location where the media was generated to avoid damage from a disaster.

3. Effectiveness of security controls for storage locations shall be tested by appropriate entities (ISO, Information Risk Management & Compliance / CRA for C&G -owned storage locations and by third-parties for third-party managed storage locations) at least annually.

4. Appropriate firefighting equipment shall be provided and suitably placed in accordance with local, state, and national laws and regulations.

PE-05 Securing Restricted Access Areas

Physical protection and guidelines for working in restricted access areas such as data centers, laboratories and storage rooms should be designed and applied, based on business needs.

Owner	Control Mapping		
Design Owner: Corporate Security and Safety, GFM Implementation Owner: Corporate Security and Safety, GFM Data Center Services, Business Groups	ISO-27001:2013 A.11.1.5	PCI-DSS 9.2	NIST 800-53 PE-1 NIST 800-53 PE-2 NIST 800-53 PE-3 NIST 800-53 PE-4 NIST 800-53 PE-7 NIST 800-53 PL-4

Last Updated: October, 2018

PE-05 Requirements

1. C&G users shall only be provided unescorted access privilege to restricted access areas where network infrastructure equipment is installed such as data centers and engineering labs based on approval from the Restricted Access Area Manager. All other individuals must be escorted.

2. Restricted access areas should be located in an area as to avoid access by, or draw unnecessary attention from the public.

3. Physical access shall be restricted to network equipment (wireless infrastructure devices etc.).

   3.1 Network equipment must be placed in a physical location that is not easily accessible to unauthorized personnel.

   3.2 Network equipment must be protected from unauthorized replacements and modification.

4. Based on the business needs, vacant restricted access areas such as data centers, lab environments and storage locations should be physically locked and the security status should be regularly checked.

5. Photography, video, audio or other recording is not allowed unless specifically authorized by the heads of the respective Business Groups.

6. Based on the business requirements, restricted access areas should use video cameras and/or access control mechanisms to monitor and log individual physical access.

6.1 Video cameras and/or access control mechanisms shall be configured to ensure they are protected from tampering or disabling.

6.2 Video cameras and/or access control logs are stored for at least 90 days where applicable.

7. References and additional requirements related to this control:

7.1 Data Center Services Acceptable Use Policy

7.2 Logical Access Control Security Standard

PE-06 Delivery and Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, if possible isolated from restricted access areas to avoid unauthorized access.

Owner	Control Mapping		
Design Owner: GFM Implementation Owner: GFM	ISO-27001:2013 A.11.1.6	N/A	NIST 800-53 PE-3 NIST 800-53 PE-7 NIST 800-53 PE-16

Last Updated: October, 2018

PE-06 Requirements

1. Access to facility delivery and loading areas from outside of the building shall be restricted to authorized personnel.

2. The delivery and loading area shall be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building.

3. The internal doors that lead to the delivery and loading area shall be secured when the external doors are opened.

4. Incoming material at restricted access areas such as data centers, engineering labs shall be registered upon entry to the location.

5. Incoming and outgoing shipments shall be physically segregated.

Equipment

PE-07 Equipment Siting and Protection

Equipment must be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Owner	Control Mapping		
Design Owner: GFM Implementation Owner: GFM	ISO-27001:2013 A.11.2.1	PCI-DSS 9.6 PCI-DSS 9.9	NIST 800-53 PE-1 NIST 800-53 PE-18

Last Updated: October, 2018

PE-07 Requirements

1. Equipment shall be sited to minimize unnecessary access into work areas.

2. Equipment at restricted access areas shall be positioned appropriately and the viewing angle must be restricted to reduce the risk of information being viewed by unauthorized persons during their use.

3. Based on the business needs, equipment should use an electrical power surge protection device that is connected in-line between the equipment, or equipment rack, and the power source.

4. The use of special protection methods, such as keyboard membranes, shall be used for equipment in environments where there is an increased risk of dust and dirt.

5. Based on the business needs, physical access control mechanisms should be in place to prevent access to storage rooms.

6. Eating or drinking should be avoided inside restricted access areas.

7. Based on the business needs and other geographic conditions, lightning protection should be applied to buildings and lightning protection filters should be fitted to all incoming power and communications lines.

8. Data center Management and Facilities shall maintain contact with local service providers in the event of fire, flood, or other emergencies.

PE-08 Supporting Utilities

Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

Owner	Control Mapping		
Design Owner: GFM Implementation Owner: GFM	ISO-27001:2013 A.11.2.2	PCI-DSS 9.9	NIST 800-53 PE-1 NIST 800-53 PE-9 NIST 800-53 PE-11 NIST 800-53 PE-12 NIST 800-53 PE-14

Last Updated: October, 2018

PE-08 Requirements

1. Supporting utilities such as electricity, water supply, sewage, heating/ventilation, and air conditioning shall be adequate for the systems they are supporting and at a minimum meet the manufacturer/vendor specifications and recommendations.

2. Access to incoming circuits to a facility shall be secure.

3. Based on the business needs, an UPS should be used, as appropriate, to support orderly shutdown or continuous operation for equipment supporting critical business operations and shall be tested according to the manufactures recommendation.

4. Power contingency plans shall address the actions to be taken in the event of UPS failure.

5. Based on the business needs, a long-term backup power option (such as a diesel or gasoline powered generator) should be in place in case of a prolonged power failure.

6. Support utilities and equipment used to provide long-term backup power shall be inspected and tested on a monthly basis to ensure proper operation and adequate capacity.

7. Should a diesel or gasoline-powered generator be used, an adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period. The fuel source should be adequately treated or replaced in such a way as to prevent deterioration.

8. Based on the business needs, emergency “power-off” switches should be located near emergency exits in equipment rooms to facilitate rapid shutdown in case of an emergency.

9. Emergency lighting shall be provided in case of main power failure according to local regulation or customs.

10. The water supply shall be stable and adequate to supply air conditioning, humidification equipment, and fire suppression systems, as required.

11. To protect information systems from damage resulting from water leakage, a master shut-off valve shall be readily accessible and known to key personnel.

12. Based on the business needs, telecommunications equipment must be connected to the utility provider by at least two diverse routes to prevent removal of voice services if there is a failure in one connection path.

PE-09 Cabling Security

Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference or damage.

Owner	Control Mapping		
Design Owner: GFM, IT Implementation Owner: GFM, IT	ISO-27001:2013 A.11.2.3	PCI-DSS 9.1.2	NIST 800-53 PE-4 NIST 800-53 PE-9

Last Updated: October, 2018

PE-09 Requirements

1. Power and telecommunications lines into information processing facilities should be underground, where applicable, or subject to adequate alternative protection.

2. Network cabling shall be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas. E.g. Power cables may be segregated from communications cables to prevent interference.

3. Clearly identifiable cable and equipment markings shall be used to minimize handling errors.

4. Access to patch panels, network wiring closets/cable rooms shall be controlled and locked at all times when unattended.

5. A documented patch list shall be used to reduce the possibility of errors.

PE-10 Equipment Maintenance

Equipment must be correctly maintained to ensure its continued availability and integrity.

Owner	Control Mapping		
Design Owner: GFM, IT Implementation Owner: GFM, IT	ISO-27001:2013 A.11.2.4	PCI-DSS 9.9	NIST 800-53 MA-2 NIST 800-53 MA-2(1) NIST 800-53 MA-6

Last Updated: October, 2018

PE-10 Requirements

1. Equipment should be maintained in accordance with the supplier/manufacturer's recommended service intervals and specifications to ensure continued availability.

2. Only authorized maintenance personnel shall carry out repairs and service equipment.

3. Maintenance records for critical equipment must be maintained according to C&G records retention policy.

4. Whenever possible, non-public information should be secured in the equipment or the maintenance personnel shall be sufficiently restricted prior to the start of any maintenance activities.

5. Maintenance that is performed by personnel without explicit authorization from Restricted Access Area Managers must be escorted.

PE-11 Removal of Assets

Asset, information or software must not be taken off-site from restricted access areas without prior authorization.

Owner	Control Mapping		
Design Owner: Business Groups, Data Center Services, IT Implementation Owner: Business Groups, Data Center Services, IT, C&G users	ISO-27001:2013 A.11.2.5	PCI-DSS 9.8	NIST 800-53 MP-5 NIST 800-53 PE-16

Last Updated: October, 2018

PE-11 Requirements

1. C&G users shall not take assets, information or software from restricted access areas without prior authorization from the supervising manager or information owner.

2. Time period for equipment removal (or moving from one location to another) from restricted access areas shall be set and management must ensure that these provisions are met.

PE-12 Physical Security of Equipment and Assets Off-Premises

Security must be applied to off-site assets taking into account the different risks of working outside C&G premises.

Owner	Control Mapping		
Design Owner: Business Groups, Data Center Services, IT Implementation Owner: Business	ISO-27001:2013 A.11.2.6	PCI-DSS 9.6	NIST 800-53 MA-4 NIST 800-53 MA-4(1)

Groups, Data Center Services, IT, C&G users			

Last Updated: October, 2018

PE-12 Requirements

1. Regardless of ownership, the use of C&G equipment and assets outside C&G premises shall be authorized by the respective business group.

2. Equipment, assets and removable media taken off the premises shall not be left unattended in public places.

3. Equipment or media that is sent outside a C&G -owned facility shall be appropriately logged, authorized by management, and sent via secured courier or other delivery method that can be tracked.

   3.1 Adequate risk management mechanisms shall be in place to protect assets off-site.

   3.2 Media in transit must adhere to C&G backup and encryption requirements.

4. Manufacturers' instructions for protecting equipment shall be observed at all times.

5. Security risks, e.g. of damage, theft or eavesdropping, may vary considerably per region and must be taken into account in determining the most appropriate information security controls.

6. References and additional requirements related to this control:

   6.1 Media Handling

   6.2 OP-06 Information Backup

   6.3 Cryptographic Controls

PE-13 Secure Disposal or Reuse of Equipment

Equipment and assets must be verified to ensure that any C&G information and licensed software has been removed or securely overwritten prior to disposal or reuse.

Owner	Control Mapping		
Design Owner: IT, GFM Implementation Owner: IT	ISO-27001:2013 A.11.2.7	PCI-DSS 9.10	NIST 800-53 MP-6

Last Updated: October, 2018

PE-13 Requirements

1. Equipment and assets must be securely disposed and/or re-used using C&G -approved disposal mechanisms.

2. Locked storage rooms or containers shall be made available for use to accommodate equipment or media awaiting disposal.

3. Highly confidential or confidential information within equipment shall be rendered unrecoverable via a secure wipe program.

4. References and additional requirements related to this control:

   4.1 Media Destruction Standard

   4.2 Media Handling

PE-14 Unattended User Equipment (e.g. information system, workstation, laptop, smartphone)

C&G users must ensure that unattended equipment are appropriately protected.

Owner	Control Mapping		
Design Owner: ISO, IT Implementation Owner: C&G users	ISO-27001:2013 A.11.2.8	PCI-DSS 9.9	NIST 800-53 PE-3 NIST 800-53 PE-5

Last Updated: October, 2018

PE-14 Requirements

1. Users must terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g. password protected screen saver).

2. Users must log off of information systems when any active sessions are completed.

3. Laptops, mobile devices or removable media containing C&G information must not be left unattended in public areas such as airports, hotels, conference facilities, or other public locations.

4. References and additional requirements related to this control:

   4.1 Mobile Devices and Teleworking

PE-15 Clear Desk and Clear Screen Requirements

Clear desk requirements for non-electronic data and removable storage media and clear screen requirements for C&G facilities must be defined and implemented.

Owner	Control Mapping		
Design Owner: ISO, IT Implementation Owner: C&G users	ISO-27001:2013 A.11.2.9	PCI-DSS 9.9	NIST 800-53 AC-11(1)

Last Updated: October, 2018

PE-15 Requirements

1. Non-public information in paper form or on removable media must be locked away when not in use.

2. Computers and terminals shall be left logged off or protected with a screen saver and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended.

3. Computers and terminals shall be protected by key locks, passwords or other controls when not in use.

4. Internal storage media in photocopier, fax, printer etc. shall be securely wiped before disposal.

5. References and additional requirements related to this control:

   5.1 Media Destruction Standard

This page is intentionally left blank.

Information Security Standard Seven: Communications Security Standard

Information Security Standard Objective	
This Information Security Standard is established to ensure correct and secure communications between information systems, network devices and services.	
Control Categories	**Controls**
Network Security Management *To ensure the protection of information in networks and its supporting information processing facilities.*	• CS-01 Network Controls • CS-02 Segregation in Networks
Information transfer *To maintain the security of information transferred within C&G and to any external entity.*	• CS-03 Information Transfer Standards and Procedures • CS-04 Agreements on Information Transfer Between C&G and External Parties • CS-05 Information Transfer Between C&G Business Groups • CS-06 Confidentiality or Non-Disclosure Agreements

Network Security Management

CS-01 Network Controls

Networks must be designed, managed, and controlled to protect information in systems and applications.

Owner	Control Mapping		
Design Owners: IT, Business Groups, ISO Implementation Owners: Business Groups	ISO-27001:2013 A.13.1.1 ISO-27001:2013 A.13.1.2	PCI-DSS 1.1.5 PCI-DSS 2.1.1 PCI-DSS 2.2.2 PCI-DSS 4.1.1 PCI-DSS 6.6 PCI-DSS 11.4 PCI-DSS 11.5 PCI-DSS 10.5.5	NIST 800-53 AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-1, SC-22, SC-23

Last Updated: October, 2018

CS-01 Requirements

1. Business/IT owners must implement controls to ensure the information security of information in networks, and the protection of connected services from unauthorized access.

2. Procedures for the management of networking equipment and protection of network services shall be defined, documented and implemented.

3. Based on the business and regulatory requirements, operational responsibility for networks should be separated from operational responsibilities of information systems.

4. Based on the criticality of information being transmitted, security controls shall be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications.

5. Information security controls shall be established and implemented to safeguard the availability of network services.

6. Information security events from network equipment and network services shall be logged and monitored.

7. Connection of non-C&G network devices to the C&G network is strictly prohibited.

8. Connection of non-approved systems to the C&G network is strictly prohibited.

9. References and additional requirements related to this control:

    9.1 Network Access Standard

    9.2 Security Zone Standard

    9.3 Bastion Host Standard

    9.4 Wireless Access Point Standard

    9.5 Information Security Continuity

    9.6 Logging and Monitoring

    9.7 AC-02 Logical Access to Network and Network Services

    9.8 Corporate Mobility Security Standard

CS-02 Segregation in Networks

Networks must be segregated to support Information Security and business requirements.

Owner	Control Mapping		
Design Owners: IT, Business Groups, ISO Implementation Owners: Business Groups	ISO-27001:2013 A.13.1.3	PCI-DSS 1.2 PCI-DSS 1.3 PCI-DSS 1.1.5 PCI-DSS 1.3.7 PCI-DSS 2.2.1 PCI-DSS 4.1	NIST 800-53 AC-4 NIST 800-53 SA-8 NIST 800-53 SC-7

Last Updated: October, 2018

CS-02 Requirements

1. Appropriate level of security controls must be applied to different network segments based on the value and classification of information stored or processed in the network, levels of trust, and lines of business to reduce the business impact and associated risks.

2. Networks must be designed and configured to filter traffic between different segments and block any unauthorized access.

3. Firewall and router configurations shall prevent any unauthorized connections between untrusted networks and any system components storing highly confidential or confidential information.

    3.1 Firewall and router configuration files shall be secured i.e. running configuration files (used for normal running of the firewalls or routers) and start-up configuration files (used when machines are re-booted) that have secure configurations.

    3.2 Rules for firewalls and routers supporting network for highly confidential information must be reviewed at least every 6 months.

4. The boundaries of each security zone must be defined, documented and implemented.

5. Wireless networks must be segregated from internal C&G network, isolated networks (such as lab networks) and private networks.

6. Servers, networks and engineering laboratory environments used for research and development and related activities must be clearly identified and segregated from other networks.

7. References and additional requirements related to this control:

   7.1 Network Access Standard

   7.2 Security Zone Standard

   7.3 Bastion Host Standard

   7.4 Firewall and VPN Standard

   7.5 AC-02 Logical Access to Network and Network Services

   7.6 Corporate Mobility Security Standard

   7.7 Information Classification

Information Transfer

CS-03 Information Transfer Standards and Procedures

Formal information transfer standards, procedures and controls must be in place to protect the transfer of information through the use of all types of communication facilities.

Owner	Control Mapping		
Design Owners: IT, Business Groups, ISO Implementation Owners: Business Groups	ISO-27001:2013 A.13.2.1	PCI-DSS 12.5.1 PCI-DSS 4.1 PCI-DSS 4.1.1	NIST 800-53 AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9

Last Updated: October, 2018

CS-03 Requirements

10. There shall be defined and documented procedures to protect exchanged information from interception, copying, modification, miss-routing, and destruction.

11. There shall be defined and documented procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communication.

12. There shall be defined and documented procedures for protecting communicated non-public electronic information that is in the form of an attachment.

13. In cases where technical information is transported or transmitted across international borders, Business/IT owners must consult with Legal to implement appropriate controls for compliance with export control laws.

14. C&G users should not compromise C&G information via impersonation, forwarding of spams and malware, unauthorized purchasing, and other inappropriate means.

15. C&G users must adhere to C&G information classification scheme for all business correspondence, including messages, in accordance with relevant national and local laws and regulations.

16. C&G users should not leave messages containing highly confidential information over voice mails as they may be accessed by unauthorized persons or communicated to unauthorized individual as a result of misdialing.

17. C&G users should use care in entering/registering C&G related data (e.g. C&G employee id, email id, etc.) in third-party software or websites, unless required by their business group for business reasons.

18. Information exchange facilities must comply with applicable law and/or regulations.

19. References and additional requirements related to this control:

    19.1 Protection from Malware

    19.2 Records Management Policy

    19.3 Records Retention Schedule

    19.4 Media Destruction Standard

    19.5 CM-01 Use of Cryptographic Controls

    19.6 AM-03 Acceptable Use

    19.7 Logical Access Control Security Standard

    19.8 Network Access Standard

    19.9 Wireless Access Point Standard

CS-04 Agreements on Information Transfer between C&G and External Parties

Agreements must address the secure transfer of business information between C&G and external parties.

Owner	Control Mapping		
Design Owners: IT, Business Groups, ISO, Legal Implementation Owners: Business Groups	ISO-27001:2013 A.13.2.2	PCI-DSS 12.3.4 PCI-DSS 9.7	NIST 800-53 CA-3 NIST 800-53 SC-9

Last Updated: October, 2018

CS-04 Requirements

1. Information exchange agreements between C&G and external parties must consider the requirements around these security concepts for inclusion, at a minimum:

    1.1 Management responsibilities for controlling and notifying data transmission, dispatch, and receipt.

    1.2 Procedures for notifying sender of data transmission, dispatch, and receipt.

    1.3 Procedures to ensure traceability and non-repudiation.

1.4 Minimum technical standards for packaging and transmission.

1.5 Escrow agreements.

1.6 Courier identification standards.

1.7 Responsibilities and liabilities in the event of Information Security incidents, such as loss of data.

1.8 Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected.

1.9 Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations.

1.10 Technical standards for recording and reading information and software.

1.11 Any special controls that may be required to protect highly confidential information, such as cryptographic keys.

2. The security content of any agreement must reflect the criticality of the business information involved, in accordance with C&G information classification scheme.

3. References and additional requirements related to this control:

3.1 Third-Party Connectivity Standard

3.2 Media Handling

3.3 Security in Supplier Relationships

CS-05 Information Transfer between C&G Business Groups

Information security controls for the secure transfer of information between C&G Business Groups must be defined and implemented.

Owner	**Control Mapping**		
Design Owners: IT, Business Groups, ISO, Legal Implementation Owners: Business Groups	ISO-27001:2013 A.13.2.2	PCI-DSS 12.3.4 PCI-DSS 9.7	NIST 800-53 CA-3 NIST 800-53 SC-9

Last Updated: October, 2018

CS-05 Requirements

1. Information security controls shall be defined and implemented for interconnection of systems or applications to transfer information between C&G business groups, including:

1.1 Restricting level of access to interconnected applications or systems based on a need-to-know basis.

1.2 Restricting the amount and type of information required by interconnected applications or systems.

1.3 Sharing known vulnerabilities of interconnected applications or systems.

1.4 Defining categories of personnel, contractors or business partners allowed using the interconnected systems and the locations from which they may be accessed.

1.5 Retention and back-up dependencies.

1.6 Fallback requirements and arrangements.

CS-06 Confidentiality or Non-Disclosure Agreements

Requirements for execution and retention of confidentiality or non-disclosure agreements reflecting C&G needs for the protection of information must be identified, regularly reviewed and documented.

Owner	Control Mapping		
Design Owners: Business/IT Owners, Global Procurement, ISO Risk Management, Legal Implementation Owners: Business Groups/IT, Global Procurement	ISO-27001:2013 A.13.2.4	PCI-DSS 7.1.3	NIST 800-53 PL-4 NIST 800-53 PS-6 NIST 800-53 SA-9

Last Updated: October, 2018

CS-06 Requirements

1. Confidentiality and non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms.

    1.1 Existing Confidentiality and Non-Disclosure Agreements templates maintained by the Legal department must be leveraged by Business groups.

2. Non-disclosure or confidentiality agreements must consider the requirements around these security concepts for inclusion, at a minimum:

    2.1 Definition of the information to be protected, in accordance with C&G information classification scheme.

        2.1.1 The Confidentiality and Non-Disclosure Agreements shall also define specific C&G information (e.g. trade secrets, specific data elements like SSN, credit card data) that must be protected.

    2.2 Expected duration of an agreement, including cases where confidentiality may need to be maintained indefinitely.

    2.3 Description of required actions to be taken, in the event of agreement termination.

    2.4 Description of responsibilities and required actions of signatories to avoid unauthorized information disclosure (such as need-to-know).

    2.5 Description of ownership of information, trade secrets and intellectual property, and how it relates to the protection of C&G information.

    2.6 Description on permitted use of C&G information, and rights of signatory to use, store or process that information.

2.7 Requirements for the right to audit and monitor activities that involve C&G highly Confidential and confidential information.

2.7.1 Such requirements should clearly specify the entity responsible for auditing and monitoring activities (external entity vs. C&G internal) related to highly confidential and confidential information.

2.8 Notification and reporting processes for information security breaches.

2.9 Terms and conditions for assets and information to be returned or destroyed at agreement cessation, in accordance with C&G approved disposal mechanisms.

2.10 Expected actions to be taken in case of breach of the confidentiality or non-disclosure agreement.

3. Confidentiality and non-disclosure agreements must be reviewed by the Legal team for compliance with all applicable laws and regulations, before engagement with the external entity.

4. Confidentiality and non-disclosure agreements must be reviewed on an annual basis and/or on occurrence of critical changes that impact these requirements.

5. Different confidential and non-disclosure agreements may be used in different circumstances, upon approval by appropriate individuals from the Legal team.

6. Master confidentiality and non-disclosure agreements with suppliers must be regularly reviewed to ensure that the requirements in those agreements are up-to-date and are applicable to all supplier entities covered under that master agreement.

7. References and additional requirements related to this control:

7.1 Management of Information Security Incidents and Improvements

7.2 Media Destruction Standard

This page is intentionally left blank.

Information Security Standard Eight: Operations Security Standard

Information Security Standard Objective	
This Information Security Standard is established to ensure the correct and secure operation of information processing facilities.	
Control Categories	**Controls**
Operational Procedures and Responsibilities *To ensure correct and secure operations of information processing facilities.*	• OP-01 Documented Operating Procedures • OP-02 Change Management • OP-03 Information System Performance Monitoring • OP-04 Separation of Information Security Zones
Protection from malware *To ensure that information and information processing facilities are protected from malware.*	• OP-05 Controls against Malware
Backup *To protect against loss of data.*	• OP-06 Information Backup
Logging and monitoring *To record events and generate evidence.*	• OP-07 Logging • OP-08 Protection of Log Information • OP-09 Clock Synchronization
Control of software installation *To ensure the integrity of production systems.*	• OP-10 Installation of Software
Technical vulnerability management *To prevent exploitation of technical vulnerabilities.*	• OP-11 Management of Technical Vulnerabilities
Information systems audit considerations *To minimize the impact of audit activities on production systems.*	• OP-12 Controlling the Use of Audit Activities
Mobile Devices and Teleworking *To ensure security during teleworking and secure use of mobile devices.*	• OP-13 Controls Specific to Mobile Devices • OP-14 Teleworking

Operational Procedures and Responsibilities

OP-01 Documented Operating Procedures

Operating procedures must be documented, have an appropriate level of access control in-place based upon a need-to-know basis, and made available to C&G users only.

Owner	**Control Mapping**		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.1.1	PCI-DSS 12.2 PCI-DSS 12.5.1	NIST 800-53 CM-1 NIST 800-53 CM-9 NIST 800-53 MA-1 NIST 800-53 MP-1 NIST 800-53 SC-1 NIST 800-53 SI-1

Last Updated: October, 2018

OP-01 Requirements

1. Documented procedures must be developed for all multi-step operational activities (such as computer start-up and close-down procedures, backup, equipment maintenance, administration, media handling, computer room and mail handling management, and safety) associated with information systems and communication facilities.

2. Access to documented procedures must be restricted on a need-to-know basis.

3. Documented procedures must include but are not limited to detailed instructions for the execution of the following activities:

   3.1 Provisioning and initial configuration of systems.

   3.2 Processing and handling of information.

   3.3 Backup of information.

   3.4 Scheduling requirements, including interdependencies with other systems, earliest time in the day for job start and latest time in the day for job completion.

   3.5 Error and exception handling, including restrictions on the use of system utilities.

   3.6 Support and escalation contacts in the event of unexpected operational or technical difficulties.

   3.7 Special output and media handling, such as management of highly confidential output including procedures for secure disposal of output from failed jobs.

   3.8 Restart and recovery of files or systems for use in the event of system failure.

   3.9 Monitoring of systems.

   3.10 Configuration management.

4. Operating procedures, and the documented procedures for system activities, must be treated as formal documents and any changes must be authorized by the respective Business/IT owner.

5. Operating procedures must be reviewed by the respective Business/IT owners at least annually and/or whenever critical changes occur.

6. If technically feasible, information systems should be managed consistently using the same procedures, tools, and utilities.

7. References and additional requirements related to this control:

   7.1 OP-06 Information Backup

   7.2 Gold Image Standard

OP-02 Change Management

Changes to C&G organization, C&G business processes, facilities, and information systems must be controlled.

Owner	Control Mapping		
Design Owner: IT, Business Groups	ISO-27002:2013 A.12.1.2	PCI-DSS 6.4 PCI-DSS 6.4.5	NIST 800-53 CM-1 NIST 800-53 CM-3

Implementation Owner: IT, Business Groups		PCI-DSS 6.4.5 PCI-DSS 6.4.5.1 PCI-DSS 6.4.5.2 PCI-DSS 6.4.5.3 PCI-DSS 6.4.5.4	NIST 800-53 CM-3(2) NIST 800-53 CM-4 NIST 800-53 CM-5 NIST 800-53 CM-9

Last Updated: October, 2018

OP-02 Requirements

1. Production systems and applications must be subject to strict change management control.

2. Changes must be categorized (such as major, significant or minor) depending on the potential impact on the availability of the system, application or data.

3. C&G change management process must include the following areas:

   3.1 Identification and recording of changes.

   3.2 Planning of changes.

   3.3 Assessment of the potential impacts, including security impacts, of such changes.

   3.4 Planning and testing of steps to roll back changes if necessary

   3.5 Formal approval procedure for proposed changes.

   3.6 Relevant communication of change details to all potentially impacted entities and individuals.

   3.7 Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes.

4. Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software or procedures.

5. All changes to production systems must be logged and those logs must be retained as per relevant standards.

6. References and additional requirements related to this control:

   6.1 Records Management Policy

   6.2 Records Retention Schedule

   6.3 IT Change Management Policy

   6.4 Patch Management Standard

   6.5 Logging and Monitoring

OP-03 Information System Performance Monitoring

The use of resources must be monitored, tuned and forecasted for future capacity requirements to ensure the required system performance and availability.

Owner	Control Mapping

Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.1.3	N/A	NIST 800-53 AU-4 NIST 800-53 AU-5 NIST 800-53 CP-2 NIST 800-53 CP-2(2) NIST 800-53 SA-2

Last Updated: October, 2018

OP-03 Requirements

1. System administrators must ensure that capacity requirements for information systems are defined so that the monitored use of resources can trigger alerts when there is a risk of breaching the requirements.

2. System tuning and monitoring must be applied to ensure, or when necessary improve, the availability and efficiency of systems.

   2.1 Detective and automated controls must be implemented and defined by the Business Groups to indicate potential problems in a timely manner.

   2.2 Projections of future capacity requirements must take into account new business and system requirements and current and projected trends in C&G information processing capabilities.

3. System administrators must monitor the utilization of key system resources including usage trends.

4. Business/IT owners must use this information to identify and plan appropriate action to avoid potential bottlenecks and dependency on key personnel that might present a threat to system security or services.

OP-04 Separation of Information Security Zones

Information Security Zones must be segregated to reduce the risks of unauthorized access or changes to the Production environment.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.1.4	PCI-DSS 6.4.1	NIST 800-53 CM-2(6) NIST 800-53 CM-5 NIST 800-53 SC-32

Last Updated: October, 2018

OP-04 Requirements

1. The level of separation required for security zones must be identified and appropriate controls must be implemented.

2. Access to data between security zones must be initiated from the more trusted security zone.

3. Access to security zones must be logged and monitored.

4. Access between security zones must be restricted on a need-to-know basis and logged as per relevant standards.

5. In instances where separation of environment or duties is difficult (e.g. development and production activities performed by same teams), other controls such as monitoring of activities, audit trails and management supervision must be implemented.

6. Servers should perform one primary function and appropriate segregation should be in place for different servers e.g. web server, database server and DNS should be on separate servers, where applicable

7. References and additional requirements related to this control:

    7.1 Logical Access Management

    7.2 Security Zone Standard

    7.3 Logging and Monitoring

Protection from Malware

OP-05 Controls against Malware

Information Security controls must be implemented to prevent, detect and recover from malware.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.2.1	PCI-DSS 1.4 PCI-DSS 5.1 PCI-DSS 5.1.1 PCI-DSS 5.1.2	NIST 800-53 AT-2 NIST 800-53 SA-8 NIST 800-53 SC-2 NIST 800-53 SC-14 NIST 800-53 SI-3 NIST 800-53 SI-7

Last Updated: October, 2018

OP-05 Requirements

1. The SIO team must define management responsibilities and procedures including details on the implementation of malware protection on systems, training in their use, reporting on their use and steps to recover from malicious code attacks.

2. Malicious code detection and repair software used to scan computers and media must be installed, patched and updated periodically.

3. Information systems must run a C&G -IT approved and managed malware protection solution. The protection solution must include:

    3.1 Desktop firewall and/or application firewall to ensure that only authorized traffic enters or leaves the information system.

    3.2 Anti-virus protection to ensure that all running software, data and/or connections are protected from malware.

    3.3 IDS/IPS to ensure that all network traffic is analyzed to ensure attacks or misuse is actively defended.

    3.4 Software control to ensure that only authorized applications and software are installed and running.

    3.5 Information system controls to ensure that only authorized connections are allowed, including limitations on the addition of unauthorized storage devices for the export of data.

    3.6 Appropriate access control to ensure only authorized personnel can access information they have a need-to-know.

4. Non-server information systems must run a C&G -IT managed and approved DLP tool to ensure proper identification of data and its protection.

    4.1 Server information systems should run a C&G -IT managed and approved DLP tool to ensure proper identification of data and its protection.

    4.2 The data protection and monitoring tool must include:

        4.2.1 Identification of data based on the information classification scheme.

        4.2.2 Central management of the policy distribution and subsequent actions.

        4.2.3 Prevention of highly confidential information being improperly stored, distributed or altered based on the policies distributed from a centrally managed DLP solution.

        4.2.4 Log and alert collection and forwarding to a centrally managed tool.

        4.2.5 The Legal department must be consulted for the usage of DLP tools in accordance with local and national regulations and laws.

        4.2.6 Appropriate access control to ensure only authorized personnel can access information they have a need-to-know.

5. Regular reviews of the software and data content of systems supporting critical business processes must be conducted.

    5.1 Presence of any unapproved files or unauthorized amendments must be formally investigated.

6. C&G -IT must implement controls to detect and prevent the access from information systems to known or suspected malicious websites (such as the use of blacklisting websites using a web gateway solution).

7. C&G -IT must implement procedures to regularly collect information on malware threats, such as subscribing to mailing lists and/or checking web sites giving information about new malwares.

    7.1 C&G -IT must verify information gathered relating to malware and ensure that warning bulletins are accurate and informative.

    7.2 C&G -IT must ensure their sources are qualified (such as reputable journals, reliable Internet sites or suppliers producing software protection against malware) and are used to differentiate between hoaxes and real malware.

    7.3 C&G -IT must have a method of determining when it is necessary to inform users of hoaxes and a process to make users aware of hoaxes that includes what to do when hoaxes are received.

8. C&G -IT must appropriately isolate environments to minimize the impact of malware on C&G infrastructure and information systems.

9. Whenever possible, anti-spyware modules must be used in the anti-virus engines.

10. Anti-virus software must scan all accessed files at all times while a system is turned on and connected to any network.

    10.1 Anti-virus software must not be disabled while a system is turned on and connected to any network.

11. References and additional requirements related to this control:

11.1 AM-03 Acceptable Use

11.2 Media Handling

11.3 IM-04 Assessment and Decision of Information Security Events.

Backup

OP-06 Information Backup

Backups must be performed and tested in accordance, as per the defined backup policy.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.3.1	PCI-DSS 9.5	NIST 800-53 CP-9 NIST 800-53 CP-9(1)

Last Updated: October, 2018

OP-06 Requirements

1. C&G -owned information systems, applications, mobile devices and data must be backed up by C&G IT using a centrally managed and approved backup solution to ensure the availability of data in the event the information system is lost, stolen, or malfunctions.

2. Archiving backups must be stored securely at a C&G -approved off-site location.

3. The C&G -IT managed and approved backup solution must ensure the following:

   3.1 Full backups are performed periodically.

   3.2 Incremental backups are performed periodically between full backups.

   3.3 Backups are stored centrally within the C&G network.

4. Backups must be accessible by ISO for investigations, data analysis or malware scanning.

5. Adequate backup facilities must be provided to ensure that all business critical information and software can be recovered following a disaster or media failure.

6. Backup processes must ensure that -

   6.1 Accurate and complete records of the backup copies and documented restoration procedures are produced.

   6.2 The extent (such as full or differential backup) and frequency of backups reflect the business requirements of C&G , the security requirements of the information involved, the data availability requirements and the criticality of the information to the continued operation of C&G .

   6.3 Backup information in all locations must be provided an appropriate level of physical and environmental protection consistent with the standards applied at the main site. Where applicable, the controls implemented on the main site must be extended to the backup site.

6.4 Restoration procedures for highly confidential information must be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

6.5 Backups storing highly confidential information must be encrypted. Cryptography keys must be retained used for backup encryption.

7. System backups must be regularly tested to ensure that they are usable, appropriately backed up and meet the requirements of the business continuity and disaster recovery plans.

8. Backups must adhere to any applicable regulatory retention requirements and any applicable C&G retention requirements.

9. Controls must be implemented to ensure that only authorized personnel can request recovery of data or files from backup.

10. References and additional requirements related to this control:

10.1 Records Management Policy

10.2 Records Retention Schedule

10.3 PE-12 Physical Security of Equipment and Assets Off-Premises

10.4 CM-01 Use of Cryptographic Controls

Logging and Monitoring

OP-07 Logging

Logs recording user activities, exceptions, faults and events must be produced, archived and appropriately reviewed.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.4.1 ISO-27002:2013 A.12.4.3	PCI-DSS 10.5.4 PCI-DSS 10.5.5 PCI-DSS 10.5.7 PCI-DSS 10.6 PCI-DSS 11.4 PCI-DSS 11.5	NIST 800-53 AU-1 NIST 800-53 AU-2 NIST 800-53 AU-3 NIST 800-53 AU-4 NIST 800-53 AU-5 NIST 800-53 AU-8 NIST 800-53 AU-11 NIST 800-53 IA-8 NIST 800-53 SC-7 NIST 800-53 SC-8 NIST 800-53 SC-9 NIST 800-53 SC-14

Last Updated: October, 2018

OP-07 Requirements

1. Appropriate level of logging and monitoring must be performed to identify, respond to, and remediate events or incidents.

2. Events may be captured at a system level, application level and/or network level.

2.1 System administrators and infrastructure groups must perform system, network and operating system level logging.

2.2 Application owners must perform appropriate logging within the application.

2.3 All responsible parties must ensure logging procedures are documented. The documentation must include:

2.3.1 Procedures for enabling and configuring logs.

2.3.2 Procedures for maintaining continuity of logging services.

2.3.3 Privileges for accessing logs.

2.4 Log content must include, when relevant:

2.4.1 User ID/Login Name

2.4.2 Source Address (Host name preferred since the IP address could change as a result of DHCP)

2.4.3 Destination Address (IP address required where available)

2.4.4 Dates, times and details of key events

2.4.5 Event name and description

2.4.6 Success or failure indication

2.4.7 Total bytes transferred

2.4.8 Connection duration

2.4.9 Files accessed and the kind of access

2.4.10 Network protocols and ports

2.4.11 Activation and deactivation of protection systems, such as anti-virus or IDS/IPS

2.4.12 Use of privileges

2.4.13 Use of system utilities

3. Logs and audit trails must not contain passwords, Personal Information, PINs, credit card data or other sensitive data.

3.1 Appropriate security and privacy controls must be implemented if the logs contain such information.

4. Wherever applicable, information system logs should be stored in a centralized location to enable centralized management.

5. Information security logs must be stored on the host for a minimum of three months and offline for a minimum of one year.

5.1 Any exceptions to this requirement must be justified by technical or operational constraints and must not affect compliance with applicable regulatory, statutory or contractual requirements.

5.2 Configuration of information systems must not overwriting the logs until the specified log retention period has passed.

6. Security monitoring of logs must take into consideration the business needs, the criticality of information, the risks to C&G assets and information, and/or any applicable security regulation or standard requirements.

7. IDS/IPS must be used to monitor all traffic at the perimeter of C&G environment as well as at critical points inside the sensitive environment.

    7.1 These systems must alert designated administrators about suspected activities and compromises.

    7.2 These systems must be regularly updated and patched.

8. File integrity monitoring tools must be used to alert system administrators of unauthorized modification of critical system files, configurations files, or content files.

9. C&G IDS/IPS managed outside the control of system and network administrators must be utilized to monitor compliance of system and network administration activities to standards and policies.

10. References and additional requirements related to this control:

    10.1 Logging Standard

    10.2 Host-based Intrusion Monitoring Standard

    10.3 OP-02 Change Management

OP-08 Protection of Log Information

Logging facilities, log archiving location and log information must be protected against tampering and unauthorized access.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.4.2	PCI-DSS 10.5.1 PCI-DSS 10.5.2 PCI-DSS 10.5.3	NIST 800-53 AU-4 NIST 800-53 AU-5 NIST 800-53 AU-9 NIST 800-53 AU-11

Last Updated: October, 2018

OP-08 Requirements

1. Access to logs, logging systems and logging facilities must adhere to C&G access control requirements.

2. Business/IT owners must implement security controls to prevent unauthorized changes to log information and to prevent operational problems with logging facilities. Such controls include:

    2.1 Alterations to the recorded message types.

    2.2 Editing or deletion of log files.

    2.3 Exceeding the storage capacity of the log file media, resulting in either the failure to record events or over-writing of past recorded events.

3. Business/IT owners must ensure that logs can be accessed by the ISO.

4. Information systems must alert designated administrators upon the failure to properly log. Appropriate and timely action must be taken by the administrator to resume system logging upon failure.

5. References and additional requirements related to this control:

   5.1 Records Management Policy

   5.2 Records Retention Schedule

   5.3 OP-06 Information Backup

OP-09 Clock Synchronization

The clocks of all information systems within C&G or security domain must be synchronized to a single reference time.

Owner	Control Mapping		
Design Owner: IT Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.4.4	PCI-DSS 10.4.1 PCI-DSS 10.4.2 PCI-DSS 10.4.3	NIST 800-53 AU-8

Last Updated: October, 2018

OP-09 Requirements

1. Information systems must synchronize system clocks with an authoritative time server.

2. A standard reference time for use within C&G must be defined.

3. Clock synchronization processes must be documented and implemented consistently.

4. Access to time data must be restricted.

5. Any changes to time settings on systems storing highly confidential or confidential information must be logged, monitored and reviewed.

6. UTC must be assigned as the time zone for all log data.

7. References and additional requirements related to this control:

   7.1 Logical Access Management

Control of Software Installation

OP-10 Installation of Software

Procedures must be implemented to control the installation of software.

Owner	Control Mapping		
Design Owner: IT, Business Groups Implementation Owner: IT, Business Groups	ISO-27002:2013 A.12.5.1 ISO-27002:2013 A.12.6.2	PCI-DSS 2.2 PCI-DSS 2.2.3 PCI-DSS 2.2.4 PCI-DSS 11.5 PCI-DSS 12.3.1 PCI-DSS 12.3.5	NIST 800-53 CM-1 NIST 800-53 CM-2 NIST 800-53 CM-3 NIST 800-53 CM-4 NIST 800-53 CM-5 NIST 800-53 CM-9

		PCI-DSS 12.3.6 PCI-DSS 12.3.7 PCI-DSS 12.6.2	NIST 800-53 SA-6 NIST 800-53 SA-7 NIST 800-53 AC-20 NIST 800-53 PL-4

Last Updated: October, 2018

OP-10 Requirements

1. Principle of least privilege and need-to-know must be applied for restricting installation of software on information systems.

2. C&G users must not have administrator access to information systems, unless required by their job function.

3. The updating of production software, applications, and program libraries must only be performed by system administrators upon appropriate management authorization.

4. Applications and operating system software must only be implemented after extensive and successful testing.

5. Information systems must run a C&G -IT centrally managed configuration tool to ensure proper management of information systems. This solution must include:

   5.1 Configuration enforcement for information systems

   5.2 Software accounting and management

   5.3 Device policy enforcement

6. All changes to applications and operating system software must adhere to all relevant change management standards.

7. Previous versions of application software must be retained as a contingency measure.

8. Wherever required, older versions of software must be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive.

9. Vendor supplied software used in production systems must be maintained at a level supported by the supplier.

10. Any decision to upgrade to a new release must take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting the version.

11. Software patches must be applied immediately if they remove or reduce major security weaknesses.

12. Physical or logical access by suppliers to information systems must only be given when necessary for support purposes.

13. Computer software relying on externally supplied software and modules must be monitored and controlled to avoid unauthorized changes, which may introduce security weaknesses.

14. References and additional requirements related to this control:

14.1 Patch Management Standard

14.2 Logging and Monitoring

14.3 Logical Access Management

14.4 Security in Supplier Relationships

Technical Vulnerability Management

OP-11 Management of Technical Vulnerabilities

Information about technical vulnerabilities of information systems being used must be obtained in a timely manner. C&G exposure to such vulnerabilities must be evaluated and appropriate controls must be implemented to address the associated risk.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: IT, Business Groups, ISO	ISO-27002:2013 A.12.6.1	PCI-DSS 6.5.1 PCI-DSS 6.5.2 PCI-DSS 6.5.3 PCI-DSS 6.5.4 PCI-DSS 6.5.5 PCI-DSS 6.5.7 PCI-DSS 6.5.8 PCI-DSS 6.5.9 PCI-DSS 6.6 PCI-DSS 11.1 PCI-DSS 11.2 PCI-DSS 11.3 PCI-DSS 11.4	NIST 800-53 RA-2 NIST 800-53 RA-5 NIST 800-53 RA-5(1) NIST 800-53 SI-2 NIST 800-53 SI-5

Last Updated: October, 2018

OP-11 Requirements

1. For effective technical vulnerability management, Business/IT owners must ensure that their asset inventory is complete and updated regularly.

2. C&G users must immediately report identification of potential technical vulnerabilities.

3. The ISO must perform technical vulnerability management, including vulnerability scanning, vulnerability monitoring, vulnerability risk assessment and any coordination activities required.

   3.1 Business/IT owners must perform asset ownership and tracking, vulnerability tracking, vulnerability remediation and patching of information systems.

   3.2 Vulnerability remediation or patching activity must be performed for high severity/high risk vulnerabilities by Business/IT owners within 90 days of the notification about vulnerabilities from the ISO.

4. The ISO Application Security team must work with the respective project teams to identify and remediate technical vulnerabilities during an application development lifecycle. Refer to Vulnerability Management Guidelines for the identification and remediation processes for technical vulnerabilities.

5. The ISO must identify business and IT risks associated with an identified vulnerability and actions to be taken.

5.1 Such actions must include:

5.1.1 Patching or fixing the identified vulnerability, or

5.1.2 Applying other compensating security controls for mitigation, or

5.1.3 Acceptance of risk by the Business/IT owner, ISO, and C&G IT Management, as applicable.

5.2 Actions listed above must be reviewed by the ISO, Business/IT owner and other stakeholders and appropriate action must be taken.

6. An audit log must be kept for all procedures undertaken to identify and remediate vulnerabilities.

7. The technical vulnerability management process must be monitored and evaluated annually, to ensure its effectiveness and efficiency.

8. High severity vulnerabilities and vulnerabilities for systems holding highly confidential data must be addressed first during remediation efforts.

9. All applications must be developed based on C&G secure coding guidelines and ISO-approved coding methodologies and tools. These are some examples of common Information Security vulnerabilities:

9.1 Injection flaws, such as SQL Injection, OS Command Injection, LDAP and XPath injection flaws, and cross-site scripting.

9.2 Buffer overflow.

9.3 Insecure cryptographic storage.

9.4 Insecure communications.

9.5 Improper error handling.

9.6 Improper access control (such as insecure direct object references, failure to restrict URL access, and directory traversal).

9.7 Cross-site request forgery (CSRF).

10. Vulnerabilities from other vulnerability sources such as OWASP Guide, SANS CWE Top 25, and CERT Secure Coding should be leveraged for vulnerability identification and remediation.

11. For public-facing web applications and web servers, new threats and vulnerabilities must be monitored and addressed on an ongoing basis. These web applications and servers must be protected against known attacks by either of the following methods:

11.1 Reviewing all public-facing web applications and servers via manual or automated application vulnerability security assessment tools or methods, at least annually and/or after any critical changes.

11.2 Installing a web-application firewall in front of public-facing web applications that contain highly confidential or confidential information.

12. The ISO must perform tests to detect presence of unauthorized wireless access points on a quarterly basis.

13. References and additional requirements related to this control:

13.1 Management of Information Security Incidents and Improvements

13.2 Information Security Reviews

13.3 Patch Management Standard

Information Systems Audit Considerations

OP-12 Controlling the Use of Audit Activities

Audit requirements and activities involving verification of production systems must be appropriately planned and agreed upon with respective entities to minimize disruptions to business processes.

Owner	Control Mapping		
Design Owner: IT, Business Groups, ISO, CRA Implementation Owner: IT, Business Groups, ISO, CRA	ISO A.12.7.1	PCI-DSS 10.5 PCI-DSS 10.5.1 PCI-DSS 10.5.2	NIST 800-53 AU-1 NIST 800-53 AU-2 NIST 800-53 PL-6

OP-12 Requirements

1. The use of audit tools during reviews for monitoring compliance with Information Security requirements must be planned and assessed beforehand to identify potential impacts to the existing IT infrastructure and information systems.

2. The scope of these reviews must be approved by the heads of the respective Business Groups, appropriate Business/IT owner and the ISO before implementation.

3. Logical tools used in these periodic reviews must be controlled to read-only and logged and monitored to produce an audit trail.

4. Individuals carrying out audits must be explicitly identified and they must be independent of the activities being audited.

5. All audit procedures, requirements, and responsibilities must be documented.

Mobile Devices and Teleworking

OP-13 Controls Specific to Mobile Devices

Information Security controls must be established and implemented to protect against the risks introduced by using mobile devices such as laptops, smartphones, and tablets.

Owner	Control Mapping		
Design Owner: ISO, IT, Business Groups Implementation Owner: Business Groups, C&G users	ISO-27002:2013 A.6.2.1	PCI-DSS 12.3.10 PCI-DSS 1.4	NIST 800-53 AC-19

Last Updated: October, 2018

OP-13 Requirements

1. C&G users in public places should ensure that their mobile devices such as laptops, smartphones, and tablets are protected from the risk of being observed by unauthorized persons.

    2.1 Screen privacy protectors may be used on mobile devices for viewing C&G information in public areas.

3. C&G users must complete corporate mobility security awareness training for increased awareness on the additional risks resulting from use of mobile devices and the Information Security controls that must be implemented.

4. Where possible, mobile devices should be carried as hand luggage and securely stored in transit.

    4.1 If required to leave a mobile device containing C&G information unattended in a vehicle, C&G users must always store it in a locked trunk when one is available.

    4.2 For vehicles without a trunk, mobile device must be stored in the luggage area and the user must ensure that it is not visible from the outside.

5. C&G mobile devices must not be left unattended, and, where possible, must be physically locked away, or authentication mechanisms (such as PIN lock or pattern lock for smartphones) must be used to secure the devices.

    5.1 For laptops, C&G password requirements must be enforced.

    5.2 For handheld devices such as smartphones and tablets; password complexity requirements must be enforced specific to the mobile platform, as defined by the ISO.

6. Use of unauthorized non-C&G mobile devices for C&G business is strictly prohibited.

7. C&G mobile devices must be able to securely wipe stored data either remotely, or locally, at will, or when the invalid credential threshold has been reached.

8. References and additional requirements related to this control:

    8.1 Corporate Mobility Security Standard

    8.2 Logging and Monitoring

    8.3 Media Destruction Standard

    8.4 Business Requirements of Logical Access Control

    8.5 Unattended User Equipment

    8.6 OP-06 Information Backup

OP-14 Teleworking

Information Security controls must be implemented to protect information accessed, processed or stored in teleworking sites.

Owner	Control Mapping		
Design Owner: ISO, IT, Business Groups, Human Resources, Legal	ISO-27002:2013 A.6.2.2	N/A	NIST 800-53 PE-17

Implementation Owner: IT, Business Groups			

Last Updated: October, 2018

OP-14 Requirements

1. The ISO Information Risk Management & Compliance team should regularly assess the effectiveness of security controls for alternate work locations involving handling of highly confidential or confidential information, where applicable based on the business needs and perceived risk.

2. References and additional requirements related to this control:

   2.1 Ways2Work Flexible Work Options

   2.2 Alternate Work Location Safety and Guidance Checklist

This page is intentionally left blank.

Information Security Standard Nine: Information System Lifecycle Security Standard

Information Security Standard Objective	
This Information Security Standard is established to ensure that Information Security is embedded across the entire information systems lifecycle.	
Control Categories	**Controls**
Information Security Requirements of Information Systems *To ensure that Information Security is an integral part of information systems across the entire lifecycle. This includes in particular specific Information Security requirements for information systems which provide services over public networks.*	• SL-01 Information Security requirements analysis and specification • SL-02 Securing information system services
Information Security in Development and Support Processes *To ensure that Information Security is designed and implemented within the development lifecycle of information systems.*	• SL-03 Secure development requirements • SL-04 Change control procedures • SL-05 Technical review after information system changes • SL-06 Information System security testing • SL-07 Information System acceptance testing
Test Data *To ensure the protection of data used for testing.*	• SL-08 Protection of test data

Information Security Requirements of Information Systems

SL-01 Information Security Requirements Analysis and Specification

Information Security controls must be included in the statements of business and technical requirements during an information system lifecycle process.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: Business Groups	ISO-27001:2013 A.14.1.1	PCI-DSS 6.3 PCI-DSS 6.3.2 PCI-DSS 6.5	NIST 800-53 SA-1 NIST 800-53 SA-3 NIST 800-53 SA-4

Last Updated: October, 2018

SL-01 Requirements

1. Information security controls must be integrated into the product/application development lifecycle process from the concept phase to the release phase for all proprietary C&G products/applications or their components.

    1.1 Information Security must be designed into all architecture layers (business, data, applications and technology) of an information system.

1.2 Information security requirements for an application must derive from various sources including, but not limited to, C&G Information Security Policy and Standards, regulatory requirements, business needs, threat identification, security incident management and vulnerability thresholds.

1.3 Information security requirements and controls must reflect the business value of the information involved and any potential negative business impact which might result from lack of adequate security controls.

2. Business/IT owners must integrate Information Security and engage ISO and the product security team in early stages of application, product or software development.

2.1 The ISO and the product security team must be engaged and involved in the review of security processes throughout the development lifecycle and in the confirmation of Information Security controls implemented by the project teams.

2.2 Use of any new technology must be analyzed by the ISO for Information Security risks and the design must be reviewed against known attack patterns.

3. Business/IT owners must document processes and procedures for secure engineering and development and provide these to respective C&G users and developers, based on their job function.

4. If products are purchased from third-party vendors, a formal acquisition process must be followed.

4.1 If the security functionality in a proposed product does not satisfy C&G Information Security requirements, the risk introduced and associated controls must be reconsidered prior to purchasing the product.

4.2 Where an additional functionality is supplied by a third-party product which possesses a security risk, the business advantage of introducing the functionality shall be weighed against the introduced risk; and security controls should be implemented to mitigate or eliminate the risk.

5. References and additional requirements related to this control:

5.1 Product Life Cycle Process

5.2 Application Security Framework and Review Process

5.3 Security in Supplier Relationships

SL-02 Securing Information System Services

Information system services must be protected from fraudulent activity, unauthorized disclosure and modification.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: Business Groups	ISO-27001:2013 A.14.1.2 ISO-27001:2013 A.14.1.3	PCI-DSS 6.5.4 PCI-DSS 6.6	NIST 800-53 SI-10 NIST 800-53 SI-7 NIST 800-53 SI-9 NIST 800-53 SI-10 NIST 800-53 AU-10 NIST 800-53 SC-7 NIST 800-53 SC-8 NIST 800-53 SC-9 NIST 800-53 SI-7 NIST 800-53 SC-14

Last Updated: October, 2018

SL-02 Requirements

1. Information system services (business-to-business connections, third-party connectivity etc.) passing over network must be authenticated and authorized.

2. There shall be an authorization process associated with who may approve contents, issuance or signing of key transactional documents.

3. Business/IT owners shall ensure that partners are fully informed of their authorizations for provision or use of the service.

4. All third-parties engaged in communication through C&G information system services shall determine and meet requirements for confidentiality, integrity, availability and non-repudiation of C&G data.

5. Confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts required must be maintained for application services passing over the network.

   5.1 Payment information supplied by a customer using services passing over the network must be verified.

   5.2 Adequate risk mitigation mechanisms to guard against fraud must be implemented for application services passing over the network.

6. Application services performing payment transactions must implement Information Security controls to avoid loss or duplication of transaction information.

7. Storage of the transaction details must be located outside of any publicly accessible environment, e.g. on a storage platform existing on C&G intranet, and not retained and exposed on a storage medium directly accessible from the Internet.

8. Wherever a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates), Information Security must be integrated and embedded throughout the entire end-to-end certificate/signature management process.

9. References and additional requirements related to this control:

   9.1 Security in Supplier Relationships

   9.2 Web Application Coding Standard

   9.3 Cryptographic Controls

Information Security in Development and Support Processes

SL-03 Secure Development Requirements

Information security controls shall be implemented for secure development.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: Business Groups	ISO-27001:2013 A.14.2.1	PCI-DSS 6.4.1 PCI-DSS 6.4.2 PCI-DSS 6.4.4	NIST 800-53 SA-1 NIST 800-53 SA-3 NIST 800-53 SA-4

Last Updated: October, 2018

SL-03 Requirements

1. C&G source code is considered highly confidential and must be protected with the highest care in accordance with C&G information classification scheme.

2. Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) must be strictly controlled to prevent the introduction of unauthorized functionality and to avoid unintentional changes in accordance with C&G access control security requirements.

3. C&G source code shall be housed in official, approved, and managed source code repositories to enable proper security oversight and controls.

   3.1 Only source code, Research & Development (R&D) information, test automation code, system documentation, and build scripts shall be stored in C&G -approved source code repositories.

   3.2 Storing source code on non-C&G approved devices is strictly prohibited. Storing source code on C&G desktops and workstations locally should be avoided.

   3.3 All source code repository servers must be authenticated via SSL certificates.

   3.4 All source code repository servers must be physically secured or encrypted.

   3.5 All cloud providers hosting C&G source code must be approved by the head of the respective Business Group, the ISO and the Cloud Enablement Council (CEC).

4. C&G source code must include the C&G copyright statement and/or use ISO-approved software watermarking. This is applicable to all C&G source code files, except for open source code or third party code which would follow its own license/copyright.

5. Servers where C&G source code is developed, built, tested or deployed must adhere to the C&G access control requirements. Access rights must commensurate with the sensitivity of the source code.

6. Security zones where C&G source code resides (e.g. development, build, test, and production environment) must be appropriately tagged by type and function.

7. After deployment of a new release in a build, test or production environment, previous releases that are not used must be removed or archived to prevent accidental re-deployment.

8. Uncompiled source code must not be stored or processed in insecure testing environments. If source code needs to be tested, it must be compiled into a binary data type, commonly known as byte code or object code.

9. Source code representing interpreted, rather than compiled data types (including shippable code) may be copied directly to lab or test environments.

10. Uncompiled source code must not be stored into the production environment from testing environments. All code written in testing environments must be considered “test only” and must not be checked into the production environment.

11. Test harness code, test cases and other instrumentation code, design documents, functional specifications and other documentary collateral must be protected in the same manner as actual application source code.

12. Compilers, editors, and other development tools or system utilities must not be accessible from production systems when not required.

13. Byte code such as Java or .NET Common Intermediate Language must be treated as source code because they can be easily reverse engineered (i.e. decompiled).

14. Open source code that has been modified for C&G distribution or third party source code licensed or adapted for C&G distribution must be treated with the same level of protection as C&G source code.

15. Source code repositories shall be periodically backed up.

16. C&G source code must be transferred and stored in C&G -approved removable devices.

17. C&G source code must be transmitted via encrypted channels.

18. When no longer in use, all data storage medium used to store source code must be decommissioned or repurposed.

19. References and additional requirements related to this control:

    19.1 Web Application Coding Standard

    19.2 Media Destruction Standard

    19.3 OP-06 Information Backup

    19.4 AM-03 Acceptable Use

    19.5 CM-01 Use of Cryptographic Controls

    19.6 Business Requirements of Logical Access Control

SL-04 Change Control Procedures

The implementation of changes for information systems must be controlled.

Owner	Control Mapping		
Design Owner: ISO, Business Groups, IT Implementation Owner: Business Groups, IT	ISO-27001:2013 A.14.2.2	PCI-DSS 6.4 PCI-DSS 6.4.5 PCI-DSS 6.4.5 PCI-DSS 6.4.5.1 PCI-DSS 6.4.5.2 PCI-DSS 6.4.5.3 PCI-DSS 6.4.5.4	NIST 800-53 CM-1 NIST 800-53 CM-3 NIST 800-53 CM-9 NIST 800-53 SA-10

Last Updated: October, 2018

SL-04 Requirements

1. Formal change control procedures for applications shall be documented and enforced by the respective Business/IT owners.

    1.1 Introduction of new systems and major changes to existing systems must follow a formal process of documentation, specification, testing, quality control, and managed implementation.

    1.2 Business Groups may follow their own set of application change control procedures. However, application change control procedures must adhere to C&G change management requirements.

2. The change control process must include a risk assessment, analysis of the impacts of changes, and specification of Information Security controls needed.

    2.1 This process must also ensure that:

2.1.1 Existing security and change control procedures are not compromised.

2.1.2 Appropriate and formal agreement and approval for changes are obtained.

3. Wherever relevant, application and production change control procedures should be integrated.

3.1 The change procedures must include:

3.1.1 Maintaining a record of agreed authorization levels.

3.1.2 Ensuring changes are submitted by authorized users.

3.1.3 Reviewing controls and integrity procedures to ensure that they are not compromised by the changes.

3.1.4 Identifying all software, information, database entities, and hardware that require amendment.

3.1.5 Obtaining formal approval for detailed proposals before work commences.

3.1.6 Ensuring authorized users accept changes prior to implementation.

3.1.7 Ensuring that the system documentation set is updated upon the completion of each change and that old documentation is archived or disposed.

3.1.8 Maintaining a version control for all software updates.

3.1.9 Maintaining an audit trail of all change requests.

3.1.10 Ensuring that operating documentation and user procedures are changed as necessary to remain up to date.

3.1.11 Ensuring that the implementation of changes takes place during a time period that does not disturb the business processes involved.

4. References and additional requirements related to this control:

4.1 Media Destruction Standard

4.2 Records Management Policy

4.3 Records Retention Schedule

4.4 IT Change Management Policy

4.5 Patch Management Standard

SL-05 Technical Review for Information System Changes

Pre and post implementation of changes to information systems must be reviewed and tested to ensure that there is no adverse impact on C&G operations or Information Security.

Owner	Control Mapping		
Design Owner: ISO, Business Groups, IT Implementation Owner: Business Groups, IT, ISO	ISO-27001:2013 A.14.2.3	PCI-DSS 6.1 PCI-DSS 6.2 PCI-DSS 11.2 PCI-DSS 11.3	NIST 800-53 CM-3(2) NIST 800-53 SI-2

Last Updated: October, 2018

SL-05 Requirements

1. There shall be a defined and documented process for review of information system changes to ensure that Information Security controls have not been compromised.

2. There shall be an annual support plan and budget to cover reviews and system testing resulting from pre and post implementation changes.

3. There shall be a defined process to ensure that notification of information systems changes is provided in time to allow appropriate tests and reviews to take place before implementation.

   3.1 Business/IT owners must notify ISO Security Architecture, Design, and Review team of information system changes for performing Information Security reviews, as applicable.

   3.2 Business/IT owners must ensure that appropriate changes are made to the business continuity plans after information systems changes.

4. If a vendor-supplier software package needs to be updated or changed, the following areas must be considered:

   4.1 The risk of built-in controls and integrity processes being compromised.

   4.2 Whether the consent of the vendor should be obtained for any changes.

   4.3 The possibility of obtaining the required changes from the vendor as standard program updates.

   4.4 The impact if C&G becomes responsible for the future maintenance of the software as a result of changes.

5. If changes are necessary, the original software must be retained and the changes must be applied to a clearly identified copy.

SL-06 Information System Security Testing

Tests of Information Security functionality must be carried out during development.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: Business Groups, ISO	ISO-27001:2013 A.14.2.8	PCI-DSS 11.2 PCI-DSS 11.3	NIST 800-53 CA-2 NIST 800-53 CA-6 NIST 800-53 CM-3 NIST 800-53 CM-4(1) NIST 800-53 CM-9 NIST 800-53 SA-11

Last Updated: October, 2018

SL-06 Requirements

1. New and updated information systems must go through security testing and verification during the development processes, including the preparation of a detailed schedule of activities, test inputs, and expected outputs under a range of conditions.

2. Initial security testing must be performed by development team for both in-house and outsourced development.

2.1 In cases where initial security testing is not possible (e.g. shrink wrap products) for vendor products, appropriate security certifications/test reports must be requested and validated from the vendor.

3. The extent of security testing must be in proportion with the criticality of information within the system.

SL-07 Information System Acceptance Testing

Acceptance testing programs and related criteria must be established for new information systems, upgrades and new versions.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: Business Groups, ISO	ISO-27001:2013 A.14.2.9	PCI-DSS 11.2 PCI-DSS 11.3	NIST 800-53 CA-2 NIST 800-53 CA-6 NIST 800-53 CM-3 NIST 800-53 CM-4(1) NIST 800-53 CM-9 NIST 800-53 SA-11

Last Updated: October, 2018

SL-07 Requirements

1. Business/IT owners shall ensure that the requirements and criteria for acceptance of new information systems are clearly defined, agreed, documented, and tested.

2. New information systems, upgrades, and new versions must only be migrated into production after obtaining formal security acceptance from the ISO and the product security team.

3. The following areas must be verified prior to formal acceptance being provided:

3.1 Preparation and testing of routine operating procedures to defined standards.

3.2 Agreed set of security controls in place.

3.3 Effective security manual procedures.

3.4 Business continuity arrangements.

3.5 Evidence that consideration has been given to the effect the new system has on the overall security of C&G .

3.6 Security training to appropriate individuals in the operation or use of new systems.

4. For major new developments, the ISO must be consulted at all stages in the development process to ensure the security of the proposed system design.

5. Appropriate tests must be carried out to confirm that all acceptance criteria have been met.

6. References and additional requirements related to this control:

6.1 Information Security Continuity

6.2 Gold Image Standard

6.3 IT Change Management Policy

Test Data

SL-08 Protection of Test Data

Production data used for testing purposes must be appropriately protected and controlled.

Owner	Control Mapping		
Design Owner: ISO, Business Groups Implementation Owner: Business Groups	ISO-27001:2013 A.14.3.1	PCI-DSS 6.4.3	NIST 800-53 Multiple controls (e.g. AC-3, AC-4)

Last Updated: October, 2018

SL-08 Requirements

1. Based on the business and regulatory requirements, the use of production data containing highly confidential or confidential data (e.g. credit card data, PII, PHI) for testing purposes must be restricted. In such cases, sensitive details and content of production data must be removed or scrubbed before use.

2. The following requirements shall be met for production data, when used for testing purposes:

   2.1 The access control procedures, which apply to production applications and systems, must also apply to test applications and systems.

   2.2 There must be separate authorization each time production data is copied to a test application system.

   2.3 Production data must be erased from a test application system immediately after the testing is complete.

   2.4 The copying and use of production data must be logged and monitored.

3. References and additional requirements related to this control:

   3.1 Logging and Monitoring

This page is intentionally left blank.

Information Security Standard Ten: Supplier Relationships Security Standard

Information Security Standard Objective	
This Information Security Standard is established for the protection of C&G information that is accessible by suppliers (third-parties, outsourced developers, vendors, business partners, other external entities).	
Control Categories	**Controls**
Security in Supplier Relationships *To ensure protection of C&G information that is accessible by suppliers.*	• SR-01 Information Security Requirements for Supplier relationships • SR-02 Addressing Security within Supplier agreements
Suppliers Service Delivery Management *To maintain an agreed level of Information Security and service delivery in line with supplier agreements.*	• SR-03 Monitoring and Review of Supplier Services • SR-04 Managing Changes to Supplier Services

Security in Supplier Relationships

SR-01 Information Security Requirements for Supplier Relationships

Information security requirements for mitigating the risks associated with supplier's access to C&G assets must be established and documented.

Owner	**Control Mapping**		
Design Owner: Global Procurement, ISO Risk Management Implementation Owner: Global Procurement, ISO Risk Management	ISO-27002:2013 A.15.1.1	PCI-DSS 12.8.1 PCI-DSS 12.8.3	NIST 800-53 CA-3 NIST 800-53 SA-9

Last Updated: October, 2018

SR-01 Requirements

1. Suppliers handling C&G data, accessing the C&G network or associating themselves with the C&G brand must go through a due diligence process prior to engagement.

2. ISO must evaluate security risks related to suppliers and identify and mandate Information Security controls to address supplier access to C&G information.

3. Procurement and ISO must identify and document the categories of suppliers' services e.g. IT services, logistics, utilities, financial services, IT infrastructure components, whom C&G allows access to its information.

4. Procurement must define a standardized process and lifecycle for managing supplier relationships following ISO standards.

5. The ISO must define the minimum security requirements for information classification and access types as the basis for individual supplier agreements based on C&G business needs and risk assessment.

6. The ISO must handle information security incidents and contingencies associated with supplier access including incident management roles and responsibilities for both C&G and suppliers.

7. There shall be defined and documented procedures for Information Security awareness and training requirements for individuals who are part of a C&G acquired entity.

   7.1 The ISO must manage any necessary transitions from the acquired entity of information, information processing facilities, ensuring that Information Security is maintained throughout the transition period.

8. In cases where third parties conduct development on behalf of C&G , these vendors must implement a development environment with an equivalent security posture as that of C&G .

   8.1 These vendors must be contractually required to provide evidence supporting this requirement at least on an annual basis or upon request.

   8.2 The business group should only engage vendors that can comply with C&G requirements.

9. Business groups must define and manage resiliency, recovery, service levels and contingency arrangements to ensure availability of information or information processing facilities provided by suppliers.

10. References and additional requirements related to this control:

    10.1 Third-Party Vendor Security Requirements Review and Monitoring Process

    10.2 Third-Party Connectivity Standard

    10.3 Third-Party Intellectual Property Policy

SR-02 Addressing Security within Supplier Agreements

Information Security requirements must be agreed upon by suppliers that may have access to, process, store, or communicate C&G information or provide IT infrastructure components.

Owner	Control Mapping		
Design Owner: Global Procurement, ISO Risk Management, Legal Implementation Owner: Global Procurement, ISO Risk Management	ISO-27002:2013 A.15.1.2	PCI-DSS 12.8.2	NIST 800-53 CA-3 NIST 800-53 PS-7 NIST 800-53 SA-9

Last Updated: October, 2018

SR-02 Requirements

1. Suppliers handling C&G data, accessing the C&G network or associating themselves with the C&G brand must have a contract in place.

2. These ISO security requirements must be considered for inclusion in supplier agreements:

   2.1 Description of information to be provided / accessed and the methods of providing/accessing the information, in accordance with C&G information classification scheme. If necessary, a mapping between C&G classification scheme and the classification scheme of the supplier will be required.

2.2 Legal and regulatory requirements, including applicable regulatory requirements, privacy and data protection, intellectual property rights and copyright, and a description of how these requirements will be met.

2.3 Obligations of each contractual party to implement an agreed set of controls (access control, performance review, monitoring, auditing etc.).

2.4 Requirements for the acceptable use of information systems and assets.

2.5 If applicable, explicit list of personnel authorized to access or receive C&G information.

2.6 Incident management requirements including reporting and responding to incidents.

2.7 Security training and awareness requirements.

2.8 Relevant regulations and security controls for sub-contractors.

2.9 Transfer of C&G information, documents, source code or information required to run C&G systems in the event of a termination of a contract.

2.10 Background screening requirements for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern.

2.11 Right to audit clause allowing C&G to audit the supplier.

2.12 Usage of data loss prevention tools.

2.13 Supplier's obligation to periodically deliver an independent report on the effectiveness of security controls and agreement on the timely correction of relevant issues discovered in the report.

2.14 Supplier's obligations to comply with C&G security requirements, as applicable.

2.15 Terms and conditions for assets and information to be returned or destroyed at agreement cessation.

3. All cloud providers must be approved by the head of the business group and cloud enablement council

4. References and additional requirements related to this control:

4.1 AM-03 Acceptable Use

4.2 Vendor Contract Security Review Process

Supplier Services Delivery Management

SR-03 Monitoring and Review of Supplier Services

C&G must regularly monitor, review and audit supplier service delivery.

Owner	Control Mapping		
Design Owner: Global Procurement, ISO Risk Management, Legal Implementation Owner: Global	ISO-27002:2013 A.15.2.1	PCI-DSS 12.8.4	NIST 800-53 PS-7 NIST 800-53 SA-9

Procurement, ISO Risk Management			

Last Updated: October, 2018

SR-03 Requirements

1. An inventory of all suppliers must be maintained by respective business groups for tracking, monitoring, compliance and reporting processes.

2. Supplier monitoring and review processes must assess if the Information Security terms and conditions of the agreements are being adhered to, and that Information Security incidents and problems are managed properly.

3. Monitoring and review process must involve a defined relationship between C&G and the supplier to:

    3.1 Provide information about Information Security incidents and review of this information by the supplier and C&G as required by the agreements and any supporting guidelines and procedures.

    3.2 Review supplier audit trails and records of Information Security events.

    3.3 Resolve and manage any identified Information Security events or incidents.

    3.4 Review Information Security aspects of supplier's supplier or sub-contractor.

4. ISO must develop and implement an annual program to monitor and measure security controls and maintain visibility into all security aspects for C&G data, accessing the C&G network.

5. The responsibility for managing service management relationship with a supplier must be assigned to a designated individual within Business/IT owner or service management team.

    5.1 Appropriate action must be taken by the Business/IT owner when deficiencies in the service delivery are observed.

SR-04 Managing Changes to Supplier Services

Changes to the provision of services by suppliers, including maintaining and improving existing Information Security policies, procedures and controls, must be managed, taking into account the criticality of business information, systems and processes involved and re-assessment of risks.

Owner	Control Mapping		
Design Owner: Global Procurement, ISO Risk Management, Legal Implementation Owner: Global Procurement, ISO Risk Management	ISO-27002:2013 A.15.2.2	PCI-DSS 6.4	NIST 800-53 RA-3 NIST 800-53 SA-9

Last Updated: October, 2018

SR-04 Requirements

1. There shall be defined and documented process for managing changes to supplier services taking into account:

1.1 Changes to supplier agreements.

1.2 Changes made by C&G to implement:

1.2.1 Enhancements to the current services offered.

1.2.2 Development of any new applications and systems.

1.2.3 Modifications or updates of C&G Information Security Policy, Standards and Technical Configuration Standards.

1.2.4 New controls to resolve Information Security incidents and to improve Information Security or physical security.

1.3 Changes in supplier services to implement:

1.3.1 Changes and enhancement to networks.

1.3.2 Use of new technologies.

1.3.3 Adoption of new products or newer versions/releases.

1.3.4 New development tools and environments.

1.3.5 Changes to physical location of service facilities.

1.3.6 Change of suppliers.

1.3.7 Subcontracting to another supplier.

This page is intentionally left blank.

Information Security Standard Eleven: Incident Management Security Standard

Information Security Standard Objective	
This Information Security Standard is established to ensure Information Security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	
Control Categories	**Controls**
Management of Information Security incidents and improvements *To ensure a consistent and effective approach to the management of Information Security incidents, including communication on security events and weaknesses.*	• IM-01 Responsibilities and procedures • IM-02 Reporting Information Security events • IM-03 Reporting Information Security weaknesses • IM-04 Assessment and decision of Information Security events • IM-05 Response to Information Security incidents • IM-06 Learning from Information Security incidents • IM-07 Collection of evidence

Management of Information Security Incidents and Improvements

IM-01 Responsibilities and Procedures

Information Security incident management roles, responsibilities and procedures must be established to ensure a quick, effective and orderly response to Information Security incidents.

Owner	**Control Mapping**		
Design Owner: ISO, SIO Implementation Owner: C&G users, SIO	ISO-27002:2013 A.16.1.1	PCI-DSS 12.5.3 PCI-DSS 12.9 PCI-DSS 12.9.1 PCI-DSS 12.9.2 PCI-DSS 12.9.3 PCI-DSS 12.9.5	NIST 800-53 IR-1 NIST 800-53 SI-4

Last Updated: October, 2018

IM-01 Requirements

1. The SIO team and the ISO must ensure that the following procedures are developed and communicated adequately within C&G :

   1.1 Procedures for incident response planning and preparation.

   1.2 Procedures for monitoring, detecting, analyzing and reporting of Information Security events and Information Security incidents.

   1.3 Procedures for logging information security incident management activities.

   1.4 Procedures for handling of forensic evidence.

   1.5 Procedures for assessment of Information Security events and assessment and determination of Information Security weaknesses.

   1.6 Procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external relevant people or organizations.

2. Information Security incident management procedures shall ensure that:

   2.1 Trained personnel handle the issues related to Information Security incidents within C&G .

      2.1.1 A 24/7 personnel shall be dedicated to respond to Information Security alerts.

   2.2 A point of contact from the IT support teams (such as desktop support, network support, data center services) and SIO teams for Information Security incidents' detection and reporting is implemented and known.

   2.3 Appropriate contacts are maintained with authorities, external interest groups or forums that handle the issues related to Information Security incidents.

3. Information Security incident management reporting procedures must include:

   3.1 Information Security event reporting forms to support the reporting action and to help document all necessary actions in case of an Information Security event.

      3.1.1 Existing IT ticketing systems should be used to support the reporting and documentation of a security incident.

      3.1.2 The ticketing systems must restrict access to incident-related tickets to specific user groups to avoid incident data to be accessible by any other legitimate user of the ticketing system.

   3.2 Procedures to be followed in case of an Information Security event, e.g. immediately noting all details such as type of non-compliance or breach, existing malfunction, screen messages and unusual behavior, and then taking care not to act alone, but to immediately report the matter to the point of contact and only take coordinated actions.

   3.3 Reference to established formal disciplinary process by Human Resources for dealing with employees who commit Information Security breaches.

   3.4 Suitable feedback processes to ensure that those persons reporting Information Security events are notified of results after the issue has been dealt with and closed.

4. The objectives of Information Security incident management at C&G shall be agreed upon with the ISO, and it must be ensured that those responsible for security incident management understand C&G priorities for handling security incidents.

   4.1 Appropriate training shall be provided to staff with Information Security incident response responsibilities.

5. System alerting and monitoring from IDS/IPS, file integrity monitoring, SIEM solution and other monitoring systems shall be performed to detect Information Security incidents.

6. For adherence to additional requirements, refer to the following standards and requirements:

   6.1 Cyber Security Incident Response Plan

   6.2 Logging and Monitoring

   6.3 HR-04 Disciplinary Process

IM-02 Reporting Information Security Events

Information security events must be reported through C&G incident reporting channels as quickly as possible.

Owner	Control Mapping		
Design Owner: ISO, SIO Implementation Owner: C&G users, ISO, SIO, IT, Business Groups	ISO-27002:2013 A.16.1.2	PCI-DSS 12.6.1a PCI-DSS 12.9 PCI-DSS 12.9.1 PCI-DSS 12.9.4	NIST 800-53 AU-6 NIST 800-53 IR-1 NIST 800-53 IR-6 NIST 800-53 SI-4 NIST 800-53 SI-5

Last Updated: October, 2018

IM-02 Requirements

1. The SIO team has been established as the point of contact for coordinating Information Security Incident Response and has the authority to take decisive actions to protect C&G assets and networks from compromise, in the event of an information security incident resulting in significant loss of data, property or brand reputation.

2. C&G users must immediately report any suspected Information Security incidents, alerts, warnings, and suspected vulnerabilities to the ISO at security@C&G .com, IT Service Desk, their management, their primary C&G point of contact, or to the SIO team.

3. Any user aware of misuse of C&G assets or IT resources shall report it to the ISO, as quickly as possible.

4. The specifics of any Information Security event or incident shall be discussed only with pertinent ISO/SIO personnel on a need-to-know basis.

   4.1 If a virus, Trojan or other malware is suspected, users must not use C&G data systems to forward such information to other users, regardless of whether the other users are internal or external to C&G .

5. C&G users shall be made aware of their responsibilities to report any Information Security events.

6. For adherence to additional requirements, refer to the following standards and requirements:

   6.1 Cyber Security Incident Response Plan

   6.2 HR-03 Information Security Awareness, Education and Training

IM-03 Reporting Information Security Weaknesses

Users of C&G information systems and services are required to report any observed or suspected Information Security weaknesses in those systems or services.

Owner	Control Mapping		
Design Owner: ISO, SIO Implementation Owner: C&G users, ISO, SIO, IT, Business Groups	ISO-27002:2013 A.16.1.3	PCI-DSS 12.9.1	NIST 800-53 IR-6 NIST 800-53 PL-4 NIST 800-53 SI-2 NIST 800-53 SI-4 NIST 800-53 SI-5

Last Updated: October, 2018

IM-03 Requirements

1. C&G users must report system, application or service vulnerabilities, weaknesses and events to the ISO at security@C&G .com, IT Service Desk, their management, their primary C&G point of contact, or to the SIO team.

   1.1 Software updates related to vulnerability remediation must be tested for complete remediation and then applied in a timely manner.

2. The reporting mechanisms shall be easily accessible and available to C&G users. The Security Incident Management Plan and other relevant documentation and details are available at Security Incident Management C&G Web Page.

3. C&G users are strictly prohibited from testing and proving security vulnerabilities, weaknesses and events, as it may be interpreted as a potential misuse of the system and could damage the information system, resulting in legal liability for individual performing the testing.

   3.1 Testing of vulnerabilities shall be only performed by designated teams with management approval and in a secure test environment (e.g. approved C&G labs).

   3.2 Testing of vulnerabilities, weaknesses and events must have a valid business reason. For example, testing of commonly known high severity vulnerability in a Windows Server affecting multiple C&G users by authorized C&G administrators under a controlled testing environment.

4. References and additional requirements related to this control:

   4.1 OP-02 Change Management

IM-04 Assessment and Decision of Information Security Events

Information security events must be assessed and decided if they must be classified as Information Security incidents.

Owner	Control Mapping		
Design Owner: ISO, SIO Implementation Owner: ISO, SIO, Business Groups	ISO-27002:2013 A.16.1.4	PCI-DSS 12.9.1	NIST 800-53 IR-4 NIST 800-53 IR-6 NIST 800-53 PL-4 NIST 800-53 SI-2 NIST 800-53 SI-4 NIST 800-53 SI-5

Last Updated: October, 2018

IM-04 Requirements

1. Upon identification of an Information Security event, the point of contact shall assess each Information Security event using the agreed Information Security event and incident severity level and decide whether the event should be classified as an Information Security incident.

2. This initial classification with details on the identified Information Security incident shall be forwarded to the SIO team for confirmation and reassessment.

3. Results of the assessment and any actions taken must be recorded in detail for the purpose of future reference and verification.

IM-05 Response to Information Security Incidents

Information Security incidents must be responded to in accordance with the documented procedures.

Owner	Control Mapping		
Design Owner: SIO Implementation Owner: ISO, SIO, Business Groups, IT	ISO-27002:2013 A.16.1.5	PCI-DSS 12.9.1 PCI-DSS 12.9.3 PCI-DSS 12.9.6	NIST 800-53 IR-7

Last Updated: October, 2018

IM-05 Requirements

1. Information Security incidents must be responded by the SIO team and other relevant individuals of C&G or external parties.

2. Information Security incident response processes must adhere to the following requirements:

   2.1 Information Security forensics analysis, as required.

   2.2 Escalation of information security incidents, as required.

   2.3 Documenting and logging all incident response activities.

   2.4 Communicating the existence of the Information Security incident or any relevant details to appropriate entities on a need-to-know basis.

   2.5 Dealing with Information Security weaknesses found to cause or contribute to the information security incident.

   2.6 Once the information security incident has been successfully dealt with, formally closing and recording it.

3. Post-incident analysis activities must take place, as necessary, to identify the source of an information security incident.

IM-06 Learning from Information Security Incidents

Knowledge gained from analyzing and resolving Information Security incidents must be used to reduce the likelihood or impact of future incidents.

Owner	Control Mapping		
Design Owner: ISO, SIO Implementation Owner: C&G users, ISO, SIO, IT, Business Groups	ISO-27002:2013 A.16.1.6	PCI-DSS 12.9.6	NIST 800-53 IR-4 NIST 800-53 IR-5 NIST 800-53 SI-4

Last Updated: October, 2018

IM-06 Requirements

1. There shall be mechanisms in place to enable the types, volumes and costs of Information Security incidents to be quantified and monitored.

2. The information gained from the evaluation of Information Security incidents shall be used to identify recurring or high impact incidents.

2.1 The evaluation of Information Security incidents may indicate a need for enhancing or implementing Information Security controls or Information Security Policy and Standard changes.

3. Lessons learned from Information Security incidents must be incorporated in the annual risk assessment and policy review process for continuous improvement of C&G Information Security posture.

IM-07 Collection of Evidence

C&G must define and apply procedures for the appropriate identification, collection, acquisition and preservation of information, which can serve as evidence.

Owner	Control Mapping		
Design Owner: ISO, SIO, Legal Implementation Owner: SIO, Legal	ISO-27002:2013 A.16.1.7	PCI-DSS A.1.4	NIST 800-53 IR-1 NIST 800-53 IR-4 NIST 800-53 IR-6 NIST 800-53 IR-7 NIST 800-53 IR-8

Last Updated: October, 2018

IM-07 Requirements

1. Internal procedures shall be developed and followed to collect and preserve evidence in a timely manner for the purposes of disciplinary actions against C&G users. Legal guidance must be sought to develop and document these procedures.

2. The procedures must take into account of:

2.1 Chain of custody.

2.2 Safety of evidence.

2.3 Safety of personnel

2.4 Roles and responsibilities of personnel involved.

2.5 Competency of personnel.

2.6 Documentation.

2.7 Briefing.

3. Forensics must only be performed on copies of the evidential material to protect the integrity of the evidential material.

4. In cases where forensics and evidence preservation is required, to avoid intentional or accidental tampering or destruction of evidence, the SIO team must involve Legal, forensics team, Human Resources (if required) and federal agencies (if required) early in the incident handling process.

5. Legal and jurisdictional boundaries and requirements shall be considered to maximize chances of admission across the relevant jurisdictions.

This page is intentionally left blank.

Information Security Standard Twelve: Information Security Continuity

Information Security Standard Objective	
This Information Security standard is established to define roles, responsibilities and requirements to mitigate the impact of interruptions to business activities and to protect critical business processes from the effects of major failures of information systems and/or significant events which threaten normal business operations, and to ensure Information Security continuity and/or resumption within accepted operational and business requirements. This Standard aligns with C&G Enterprise Resiliency and Technology Availability Policy.	
Control Categories	**Controls**
Information Security Continuity *Information security continuity must be embedded in C&G enterprise resiliency and technology availability processes to ensure protection of information at any time and to anticipate adverse occurrences.*	• IC-01 Planning Information Security Continuity • IC-02 Implementing Information Security Continuity • IC-03 Verify, Review and evaluate Information Security Continuity
Redundancies *To ensure availability of information processing facilities.*	• IC-04 Availability of Information Processing facilities

Information Security Continuity

IC-01 Planning Information Security Continuity

C&G must determine requirements for continuity of Information Security in adverse situations, e.g. during a crisis or a disaster.

Owner	**Control Mapping**		
Design Owner: ISO Enterprise Resiliency, Business Groups Implementation Owner: ISO Enterprise Resiliency, Business Groups	ISO-27002:2013 A.17.1.1	PCI-DSS 12.1.2 PCI-DSS 12.9.1	NIST 800-53 CP-1 NIST 800-53 CP-2 NIST 800-53 CP-4 NIST 800-53 CP-10

Last Updated: October, 2018

IC-01 Requirements

1. C&G must establish an Enterprise Resiliency Organization, staff it with appropriate dedicated resources and identify and assign stakeholders from all critical business functions to participate in the program.

2. The ISO Enterprise Resiliency Organization must define, document and implement procedures for:

    2.1 Capturing Information Security aspects in the business continuity and disaster recovery processes. They must consider the following aspects, at a minimum:

        2.1.1 Information security roles and responsibilities, in the event of a disaster.

        2.1.2 Acceptable loss to availability of information and services, in the event of a disaster.

2.1.3 Implementation and maintenance of Information Security controls or compensating controls, in the event of a disaster.

2.2 Performing a business impact analysis considering C&G metal classification systems for applications to ensure that Information Security aspects in adverse situations have been identified.

2.3 Identifying an adequate management structure to prepare for, mitigate and respond to a disruptive event using representatives from various Business Groups with necessary authority, experience and competence.

2.4 Identifying and working with a point of contact in Corporate Security and Safety (for general incidents) and the SIO team (for Information Security incidents) to manage an incident and maintain Information Security, in the event of a disruptive event.

2.5 Developing documented plans and response and recovery procedures detailing how C&G should manage a disruptive event and should maintain its Information Security to a pre-determined level, in accordance with the Information Security Policy and Standards and C&G executive managements' expectations.

2.6 Identifying processes and procedures to maintain Information Security controls or implement compensating controls for Information Security controls that cannot be maintained, during an adverse situation.

3. References and additional requirements related to this control:

3.1 Enterprise Resiliency and Technology Availability Policy

IC-02 Implementing Information Security Continuity

C&G must establish, document, implement and maintain processes, procedures and controls to guarantee the required level of continuity for Information Security during an adverse situation.

Owner	Control Mapping		
Design Owner: ISO Enterprise Resiliency, Business Groups Implementation Owner: ISO Enterprise Resiliency, Business Groups	ISO-27002:2013 A.17.1.2	PCI-DSS 12.9.1	NIST 800-53 CP-1 NIST 800-53 CP-2 NIST 800-53 CP-4 NIST 800-53 CP-10

Last Updated: October, 2018

IC-02 Requirements

1. The ISO Enterprise Resiliency team must provide a framework and appropriate guidance to Business/IT owners for conducting Business Impact Analysis (BIA) and ensuring that processes and procedures are implemented to guarantee the required level of continuity for Information Security during an adverse event.

2. Business/IT owners must implement adequate recovery plans for their business processes, their critical vendor processes, and supporting information systems.

2.1 Emergency procedures, manual fallback plans, and resumption plans for the applications shall be defined, documented and implemented.

2.2 Fallback arrangements for alternative technical services, such as information processing and communications facilities from service providers shall be identified and implemented.

3. Business continuity and disaster recovery plans must include a list of all employees (with name, job title, and contact information) on the recovery team, step-by-step tasks to be executed, critical contact list and any supporting documentation and diagrams.

4. Business continuity and disaster recovery plan must describe the approach for continuity, for example the approach to ensure information or information system availability and Information Security.

5. Business continuity and disaster recovery plan must also specify the escalation plan and the conditions for its activation, as well as the individuals responsible (with name, job title, and contact information) for executing each component of the plan.

6. Business continuity and disaster recovery plan must include procedures for recovering from Information Security incidents (e.g. malware attacks, virus outbreak, denial of service attacks), including all necessary data and software backup and recovery arrangements.

7. References and additional requirements related to this control:

   7.1 Enterprise Resiliency and Technology Availability Policy

IC-03 Verify, Review and Evaluate Information Security Continuity

C&G must verify the established and implemented Information Security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.

Owner	Control Mapping		
Design Owner: ISO Enterprise Resiliency, Business Groups Implementation Owner: ISO Enterprise Resiliency, Business Groups	ISO-27002:2013 A.17.1.3	PCI-DSS 12.9.2	NIST 800-53 CP-2 NIST 800-53 CP-4 NIST 800-53 CP-4(1)

Last Updated: October, 2018

IC-03 Requirements

1. Business continuity and disaster recovery plan must be tested at least annually to determine effectiveness, adequacy and timely performance against C&G business continuity objectives and the following aspects:

   1.1 Initial response capability.

   1.2 Coordination between incident response and business continuity efforts.

   1.3 Functional recovery plans.

2. These tests must ensure that all members of the recovery team and other relevant users are aware of the plans and their responsibility for business continuity and Information Security and know their role when a plan is invoked.

3. The test schedule for business continuity and disaster recovery plan must indicate how and when each element of the plan should be tested.

   3.1 Each element of the plan(s) must be tested at least once during a three-year period.

4. These tests must review the validity and effectiveness of Information Security continuity controls when Information Security processes, controls, business continuity or disaster recovery processes change.

5. A variety of techniques can be used to provide assurance that the plan(s) will operate during a real event. These should include:

   5.1 Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions e.g. malicious code attacks, natural disaster).

   5.2 Simulations (particularly for training people in their post-incident/crisis management roles).

   5.3 Technical recovery testing (ensuring information systems can be restored effectively).

   5.4 Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site).

   5.5 Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment).

   5.6 Complete rehearsals (testing that C&G personnel, equipment, facilities, and processes can cope with interruptions).

6. The results of these tests and the actions taken to improve the plans must be documented. Identified gaps in the plan must be remediated and re-tested within 90 days of the original test date.

7. Responsibility must be documented and assigned for regular reviews of each business continuity plan.

8. Changes in business or IT processes not reflected in the business continuity plans must be followed by an appropriate update of the plan.

   8.1 The formal change control process must ensure that the updated business continuity plans are distributed and reinforced by regular reviews of the plan.

   8.2 Changes where updating of business continuity and disaster recovery plans must be considered are acquisition of new equipment, upgrading of systems and changes in:

      8.2.1 Personnel and personnel levels.

      8.2.2 Addresses or telephone numbers.

      8.2.3 Business strategy.

      8.2.4 Location, facilities, and resources.

      8.2.5 Regulatory requirements.

      8.2.6 Contractors, suppliers, and key customers.

      8.2.7 Processes, new or withdrawn ones.

      8.2.8 Operational and financial risk.

9. References and additional requirements related to this control:

   9.1 Enterprise Resiliency and Technology Availability Policy

Redundancies

IC-04 Availability of Information Processing Facilities

Information processing facilities must be implemented with redundancy sufficient to meet availability requirements.

Owner	Control Mapping		
Design Owner: ISO Enterprise Resiliency, Business Groups Implementation Owner: ISO Enterprise Resiliency, Business Groups	ISO-27002:2013 A.17.2.1	PCI-DSS 12.1.2	NIST 800-53 CP-6 NIST 800-53 CP-7

Last Updated: October, 2018

IC-04 Requirements

1. Based on the criticality of an application, information within the application, business requirements and business risks; availability requirements (Recovery Time Objective and Recovery Point Objective) for the application must be identified.

2. For Platinum and Gold applications, redundant components or architectures must be maintained to ensure availability of information. (Product Classification Definitions need to be defined).

3. Redundant components or architectures must implement and maintain Information Security controls or compensating controls similar to the existing components or architectures.

4. For Platinum and Gold applications, all elements of the redundant information systems must be tested annually to ensure the failover from one component to another component works as intended.

5. References and additional requirements related to this control:

   5.1 Enterprise Resiliency and Technology Availability Policy

This page is intentionally left blank.

Information Security Standard Thirteen: Compliance Security Standard

Information Security Standard Objective	
This Information Security Standard is established to assure compliance with applicable law, statutory, regulatory, applicable security contractual requirements, and of any Information Security requirements.	
Control Categories	**Controls**
Compliance with Legal and Contractual Requirements *To avoid breaches of legal, statutory, regulatory or contractual obligations related to Information Security and of any security requirements.*	• CO-01 Identification of Applicable Laws and Contractual Requirements • CO-02 Intellectual Property Rights (IPR) • CO-03 Protection of Documented Information • CO-04 Privacy and Protection of Personal Information • CO-05 Regulation of Cryptographic Controls
Information Security Reviews *To ensure that Information Security is implemented and operated in accordance with C&G Information Security Policy and Standards*	• CO-06 Independent Review of Information Security • CO-07 Technical Compliance Inspection

Compliance with Legal and Contractual Requirements

CO-01 Identification of Applicable Laws and Contractual Requirements

All applicable statutory, regulatory, applicable security contractual requirements and C&G process and resources to meet these requirements must be identified, documented and kept up to date for each information system and C&G .

Owner	**Control Mapping**		
Design Owner: ISO, Legal Implementation Owner: Global Procurement, Business Groups	ISO-27002:2013 A.18.1.1	PCI-DSS 12.5.1	NIST 800-53 XX-1 Controls

Last Updated: October, 2018

CO-01 Requirements

1. Business Groups are responsible for the compliance with regulatory and legal requirements for their information systems.

   1.1 Business Group, for each of their information systems, is responsible to ensure compliance with statutory, regulatory, legal requirements and contractual requirements globally.

   1.2 They are responsible to define and maintain up-to-date documentation relevant to demonstrate their compliance with the Information Security requirements.

   1.3 Information assets may include data, objects, applications, infrastructure and hardware.

1.4 The following are selected examples of Information Security laws, regulations and industry standards that may be applicable to certain business activities, products and/or services. (This is not meant to be a comprehensive list of law and regulation applicable to C&G .)

1.4.1 Gramm-Leach-Bliley Act (GLBA).

1.4.2 PCI-DSS. Refer to PCI DSS Guidelines and contact ISO for additional information regarding PCI compliance.

1.4.3 Health Insurance Portability and Accountability Act.

1.4.4 Sarbanes Oxley Act (SOX)

1.4.5 Federal Information Security Management Act (FISMA) and Federal Risk and Authorization Management (FedRAMP)

2. Export controlled material must be classified as Highly Confidential information and must be protected in accordance with applicable regulatory/trade compliance requirements and C&G information classification scheme.

3. Specific controls and responsibilities to meet statutory, regulatory, and contractual requirements must be defined and documented by the respective business groups, with the support of the ISO.

CO-02 Intellectual Property Rights (IPR)

Appropriate procedures must be implemented to ensure compliance with applicable laws, statutory, regulatory, and applicable security contractual requirements for the use of material in respect to Intellectual Property Rights and the use of proprietary software products.

Owner	Control Mapping		
Design Owner: ISO, Legal Implementation Owner: Global Procurement, Business Groups	ISO-27002:2013 A.18.1.2	PCI-DSS 12.3.1 PCI-DSS 12.3.5 PCI-DSS 12.3.7	NIST 800-53 SA-6

Last Updated: October, 2018

CO-02 Requirements

1. All C&G organizations, employees and contractors are responsible to comply with legal requirements regarding Intellectual Property use and rights including, but not limited to, copyright, design rights, trademarks.

2. Software must be acquired after proper vetting of the supplier by the Global Procurement team in accordance with the procurement process.

3. Business groups and IT owners must implement procedures to protect intellectual property rights of the assets within their area of responsibility. The procedures must include the following areas -

3.1 Maintenance of appropriate licensing conditions of that asset.

3.2 Secure disposing or transferring software to others.

3.3 Restriction on duplication, conversion to other formats, or copying in full or part other than permitted by copyright law.

4. C&G IT and/or the respective Business Group must conduct periodic reviews to ensure that only authorized software products are installed, licensing conditions are met and maximum number of users permitted for the usage of software is not exceeded.

5. In the event of non-compliance with copyright and software licensing requirements by a C&G user, appropriate disciplinary actions must be taken.

6. References and additional requirements related to this control:

   6.1 Media Destruction Standard

   6.2 AM-03 Acceptable Use

   6.3 HR-04 Disciplinary Process

   6.4 Global Procurement Policy

CO-03 Protection of Documented Information

Records must be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with applicable laws, statutory, regulatory, and applicable security contractual requirements.

Owner	Control Mapping		
Design Owner: ISO, Legal Implementation Owner: Global Procurement, Business Groups	ISO-27002:2013 A.18.1.3	PCI-DSS 12.3.4 PCI-DSS 9.7.1 PCI-DSS 9.6 PCI-DSS 10.5.1 PCI-DSS 10.5.2	NIST 800-53 AU-9 NIST 800-53 AU-11 NIST 800-53 CP-9 NIST 800-53 MP-1 NIST 800-53 MP-4 NIST 800-53 SA-5 NIST 800-53 SI-12

Last Updated: October, 2018

CO-03 Requirements

1. Records (in both physical and electronic form) shall be stored and protected in accordance with C&G retention requirements and applicable statutory, regulatory and contractual requirements.

2. Records may be categorized based on information classification and/or business area e.g. financial records, audit records, transactional logs, server logs, database logs. The classification must be established by the record owner.

3. Records storage, handling and maintenance procedures shall be defined, documented and implemented with the following inclusions:

   3.1 Retention requirements and applicable statutory, regulatory and applicable contractual requirements to provide support for after-the-fact investigations of Information Security incidents.

   3.2 Storage and retention of cryptographic keying material associated with the records.

   3.3 Deterioration of media used for storage of records.

   3.4 Protection of records from loss, falsification and destruction.

      3.4.1 Based on the criticality of records, cryptographic mechanisms must be used for protection of records.

3.5 Logical and physical access restriction for records.

4. Records storage technologies shall clearly identify records and their retention period and implement appropriate security controls after the retention period to destruct data.

5. References and additional requirements related to this control:

   5.1 Records Management Policy

   5.2 Records Retention Schedule

   5.3 CM-01 Use of Cryptographic Controls

   5.4 Logical Access Control Security Standard

   5.5 Media Destruction Standard

CO-04 Privacy and Protection of Personal Information

Privacy and protection of Personal Information must be ensured as required by applicable laws, statutory, regulatory and applicable security contractual requirements.

Owner	Control Mapping		
Design Owner: ISO, PPO Implementation Owner: Business Groups	ISO-27002:2013 A.18.1.4	PCI-DSS 12.6.1a	NIST 800-53 PL-5 NIST 800-53 SI-12

Last Updated: October, 2018

CO-04 Requirements

1. Information Security controls for data privacy and protection of Personal Information shall be implemented in accordance with the Global Privacy Policy.

2. The ISO team should work in collaboration with Legal and CRA teams to ensure that data privacy and protection requirements are communicated to respective IT and business groups during the development and operations of C&G information systems. IT and business groups are responsible to implement the proper controls that will satisfy compliance to the global privacy policy requirements.

3. Business/IT owners are ultimately responsible for the enforcement of the Global Privacy Policy and implementation of technical controls to protect Personal Information.

4. During the development of a new IT application or changes to an existing IT application handling Personal Information, a privacy subject matter specialist shall be assigned to provide guidance on privacy requirements and privacy related questions.

5. Periodic privacy reviews may be performed by the CRA at their discretion to monitor compliance with privacy laws (e.g. Safe Harbor), regulatory and contractual requirements.

6. Individuals may contact C&G through the Privacy Mailbox at privacy@C&G .com or through C&G customer support, for privacy support and questions.

CO-05 Regulation of Cryptographic Controls

Cryptographic controls must be used in compliance with applicable laws, statutory, regulatory, and applicable security contractual requirements.

Owner	Control Mapping		
Design Owner: ISO, Legal Implementation Owner: Business Groups	ISO-27002:2013 A.18.1.5	PCI-DSS 8.4 PCI-DSS 2.3 PCI-DSS 4.1 PCI-DSS 4.1.1	NIST 800-53 IA-7 NIST 800-53 SC-13

Last Updated: October, 2018

CO-05 Requirements

1. All cryptographic controls shall comply with applicable local and national government regulations and export control requirements.

2. Periodic reviews shall be performed by the ISO Information Risk Management & Compliance team to monitor usage of cryptographic controls.

3. The ISO team should be consulted for guidance on the identification and implementation of cryptographic controls.

4. The Legal team must be consulted and authorized the movement, enabling controls and technologies of encrypted information or implementation of cryptographic controls across jurisdictional borders.

5. References and additional requirements related to this control:

   5.1 CM-01 Use of Cryptographic Controls

Information Security Reviews

CO-06 Independent Review of Information Security

Information Security and its implementation (i.e. control objectives, controls, policies, processes and procedures for Information Security) must be reviewed independently periodically or on any critical changes to the management of Information Security and the implementation.

Owner	Control Mapping		
Design Owner: ISO Implementation Owner: CRA, ISO	ISO-27002:2013 A.18.2.1	PCI-DSS 11.1 PCI-DSS 11.2	NIST 800-53 CA-2 (1) NIST 800-53 CA-7 NIST 800-53 SP-800 39 NIST 800-53 SP-800 37

Last Updated: October, 2018

CO-06 Requirements

1. The CRA shall conduct annual independent reviews of Information Security at C&G . These independent reviews shall ensure continuing suitability, adequacy and effectiveness of C&G approach to manage Information Security.

   1.1 The ISO Information Risk Management & Compliance team shall conduct independent reviews for Information Security certifications (e.g. ISO 27000) for Business Groups, where applicable.

2. Independent reviewers must execute internal Information Security reviews within IT or other Business Groups to evaluate the effectiveness of the control environment and its effectiveness to reduce risk to C&G assets.

3. The head of the respective Business Group must ensure that that these reviews are carried out by groups and/or individuals independent of the area under review.

4. The review must include development of a review/audit plan that describes the scope of the review and acceptance by the audited group including:

   4.1 List of Information Security controls under review

   4.2 Review procedures (sampling methodology, schedule of engagement, etc.) to be used to determine Information Security control effectiveness

   4.3 Review environment team and roles and responsibilities

5. The results of the independent review when performed by the CRA must be recorded and reported to the Audit Committee and/or the heads of the respective Business Group who initiated the reviews. The result of the Information Security review, when performed by the ISO, must be reported to the C&G Security Council, and/or the head of the respective business group in scope to the review.

   5.1 Records of the independent review must be securely maintained.

   5.2 Appropriate corrective actions shall be taken by the heads of the respective Business Group initiating the review to mitigate the risks associated with the identified deviations to C&G security requirements.

   5.3 Corrective actions and the related activities must be assigned to a designated owner. The designated owner shall be responsible for the tracking, implementation and reporting of the assigned corrective actions.

6. The ISO must engage a qualified assessor to validate compliance with the PCI-DSS on an annual basis. The annual results of the assessment must be reported to the Audit Committee.

7. The CRA and the ISO are responsible for regulatory audits with external components, as applicable, by:

   7.1 Facilitating the interaction between the Business Group and/or IT and the external auditor.

   7.2 Ensuring documentation requested by the external auditor is appropriate and provided in a timely manner as defined in the audit plan.

8. References and additional requirements related to this control:

   8.1 Security Risk and Compliance Assessments/Audit Process

   8.2 Records Management Policy

   8.3 Records Retention Schedule

CO-07 Technical Compliance Inspection

Information systems must be regularly inspected for compliance with C&G Information Security Policy and Standards.

Owner	Control Mapping

Design Owner: ISO Implementation Owner: ISO (Primary) and Business Groups on *'as needed basis'*	ISO-27002:2013 A.18.2.3	PCI-DSS 11.2 PCI-DSS 11.3	NIST 800-53 CA-2 (1) NIST 800-53 CA-7 NIST 800-53 RA-5

Last Updated: October, 2018

CO-07 Requirements

1. The ISO shall define, document and implement processes to perform technical compliance checks for monitoring adherence with Information Security Policy and Standards. Technical compliance includes Such processes must include, at a minimum:

   1.1 Methodology and scope for performing reviews.

   1.2 Measurement (e.g. Key Risk Indicators) and monitoring procedures.

   1.3 Reporting and approval procedures.

2. IT and business groups shall use technical compliance inspections to maintain compliance to applicable Information Security Policy and Standards. Reviews shall be performed by the ISO team in collaboration with C&G IT and Business Groups to monitor technical compliance of information systems with C&G Information Security Policy and Standards as appropriate based on applicable requirements annually and after any critical changes (infrastructure or environment). These reviews may be performed including but not limited to via network scanning, penetrating testing, vulnerability assessments and other periodic compliance checks.

   2.1 These technical compliance checks must be performed by competent and authorized individuals.

   2.2 For information systems under PCI scope, external vulnerability scans must be performed via an approved scanning vendor, approved by the PCI SSC, quarterly and/or in the event of a critical change impacting Information Security of the systems.

3. All non-compliance and vulnerabilities must undergo an impact analysis to determine the scope and business impact of the identified non-compliance.

4. In cases where non-compliance and associated risks are accepted, the following requirements must be met:

   4.1 Such non-compliance must be formally approved by the heads of the respective Business Group and the ISO and well-documented.

      4.1.1 Risk acceptance of this non-compliance must be based on a valid business reason.

      4.1.2 Compensating controls to lower the risks related to the non-compliance must be considered.

      4.1.3 Such non-compliance must be reviewed on an annual basis for changes in business impact or C&G ability to mitigate the associated risks.

5. Based on the business impact of the non-compliance, prioritized corrective actions must be determined and implemented.

6. Implemented corrective actions must be documented and progress must be reported on a regular basis to the ISO Management, the head of the respective Business Group and/or the CRA team, as applicable.

7. References and additional requirements related to this control:

7.1 Risk Acceptance Process

This page is intentionally left blank.

Appendix

Definitions

Definitions	
Asset	Anything that has value to C&G (e.g. information, software, hardware, services).
Asset Owner	Individual/Group accountable for the safe and secure custody, transport, storage of the asset and implementation of Information Security controls.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Business Continuity (BC)	Activity performed by C&G to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Confidential Information	Confidential information is the second highest information classification. Unauthorized disclosure, compromise, or destruction of this information would - directly or indirectly - result in an adverse impact on C&G , its customers or employees. Adverse impacts may include, but are not limited to financial loss, damage to C&G reputation and brand, loss of business, jeopardy to the security of C&G assets, and potential legal action. (Refer to the Information Classification and Handling Standard for additional details).
Contingent worker, vendor, contractor, suppliers, consultants, 3rd party employees, external parties	Any individual with access to C&G network, who is not a full time C&G employee, but has a signed a non-disclosure agreement and is in contract with C&G to provide a product or service. This includes but it is not limited, to vendors, contractors, suppliers, consultants and 3rd party employees.
Control	Means of managing risk of administrative, technical, management or legal nature. Control is used as a synonym for safeguard or countermeasure.
Critical Change(s)	Critical changes are changes that significantly impact the operations of C&G organization, business or IT. Examples of such changes include modification of IT infrastructure elements (E.g. new data center, asset addition/deletion, etc.), business changes (mergers/acquisitions/reorganization)
Disaster Recovery (DR)	Process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to C&G after a natural or human-induced disaster.
Duties	Actual job roles and responsibilities for an individual to complete his tasks. The separation of these roles and responsibilities distributing the tasks and associated privileges for a specific business process among multiple users.
Encryption	The process of transforming readable data (plaintext) into a form that is unreadable (cipher text) by all except the authorized person(s) possessing the correct key to decrypt the data.
Endpoint	Endpoint devices are Internet-capable physical assets that can connect to C&G network E.g. Laptops, workstations, desktops, servers.
Equipment	An asset, tool, appliance used for special purpose such as maintenance, administration, etc.
External	This network super zone must only host all the devices and servers that directly or indirectly serve internet facing customers for public access
Fallback Arrangements	Fallback arrangements or contingency arrangements are business procedures and measures that are executed when events (such as a disaster, malware outbreak) trigger execution of C&G Business Continuity or a Disaster Recovery Plan.

Highly Confidential Information	Highly Confidential information is the highest level of classification. Unauthorized disclosure, compromise, or destruction of this information would have a direct negative impact on C&G , its customers or employees in terms of any of the following: brand damage, significant financial loss or penalties, stock value and day-to-day operations. It is intended solely for privileged and predetermined use within C&G . (Refer to the Information Classification and Handling Standard for additional details).
Identity and Access Management	Management of access, authorization and authentication for business processes, information systems, facilities and information assets.
Information Processing Activities	IT, administrative or maintenance activities performed in data centers, storage locations, office spaces and other information processing facilities.
Information Processing Facility	Any information processing system, service or infrastructure, or the physical location housing them. E.g. data center, servers, server racks.
Information Security/Security	Preservation of confidentiality, integrity and availability of information both physically and logically.
Information Security Breach	A security breach is defined as any adverse security event that results in unauthorized access to IT infrastructure and/or impermissible acquisition, access, use or disclosure that compromises the confidentiality, integrity or privacy of Highly Confidential Information (e.g. Personal Information, Cardholder Data)
Information Security Event	An identified occurrence of a system, service or network state indicating a possible violation of the Information Security policy or failure of safeguards, or a previously unknown situation that may be Information Security relevant.
Information Security Incident	An Information Security incident is made up of one or more unwanted or unexpected Information Security events that could compromise the confidentiality, integrity or availability of C&G information and weaken or impair business operations.
Information Security Policy	Guiding principles used to set direction in C&G and to communicate management's expectations of how C&G should operate.
Information Systems	Integrated set of components for collecting, storing, and processing information. Information systems include assets, mobile devices, workstations, desktops, servers, etc.
Integrity	Protection of the accuracy and completeness of information.
Intellectual Property	A formula, process, design or information that has business, intellectual or informational value for C&G . This includes trade secret, source code, proprietary information/software, industrial design, trademark, patents, intangible assets etc.
Intellectual Property Rights (IPR)	Intellectual property rights are a bundle of exclusive legal rights over creations of the mind, both artistic and commercial. The former is covered by copyright laws, which protect creative works and gives the copyright holder exclusive right to control reproduction or adaptation of such works for a certain period of time. The second category is collectively known as "industrial properties", as they are typically created and used for industrial or commercial purposes and may include a patent, trademark, industrial design, trade secret, source code and proprietary information and/or knowledge.
Internal	This network must host only host all devices and servers that directly or indirectly provide services to customers from within C&G networks.
Key Management Activities	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.
Laboratories	C&G office space or room used for research and development, testing and other critical engineering activities involving highly confidential information or confidential information.

	Labs may contain UAT, QA, DEV, Support network segments as well as Lab infrastructure devices (servers, consoles, etc.) where applicable.
Least Privilege	Requirements where an individual must be able to access only the assets, facilities or information that are required and authorized for his job role or function.
Lifecycle for Application/Product/System Development	A lifecycle is a series of steps or phases that provide a framework for the development of an information system, application, product or software. E.g. waterfall process or agile development methodologies.
Mobile device	A physical removable and/or portable device such as laptops, smartphones and tablets.
Need-to-know	Predetermined criteria (based on business needs) on the basis of which access is restricted to an information systems, facilities or information assets. Unless a user has a valid business reason to access the information system, facility or information asset, his access is denied.
Network Service Provider	Internal Business Group, external organization or part of an external organization that manages and delivers a network service or services to C&G .
Payment Card Industry (PCI)– Data Security Standard	PCI Data Security Standard (PCI DSS) is an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
PCI Qualified Security Assessor	Qualified Security Assessor (QSA) companies are organizations that have been qualified by the PCI DSS Council to have their employees assess compliance to the PCI DSS standard. Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI DSS.
Penetration Test	A penetration test is a method of evaluating the Information Security of a computer system or network by simulating an attack by a malicious user
Personal Information	Personal Information is any information related to any identified or identifiable natural person, such as C&G personnel, customers, subcontractors, partners or any other third party (including third parties" personnel). Examples of Personal Information are name, address, credit card number, but also IP Address, browsing history and purchasing history. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his identity.
Private Information	Private information is primarily internal or proprietary information not meant for public knowledge or disclosure. Unauthorized disclosure, compromise, or destruction would result in some adverse impact to C&G , its customers, or employees. (Refer to the Information Classification and Handling Standard for additional details).
Privilege/Privileged Access/Accounts	Privilege is special access or rights granted to an individual. Privileged accounts are generally those accounts that have one or more of the following capabilities: • Ability to grant access to any other account • Ability to change / manage accounts • Ability to access or modify production applications, databases, operating systems, network parameters or any other system configurations • Ability to access or modify C&G non-public information However, not all accounts that meet the capabilities above may be considered privileged accounts in all scenarios (e.g., an account that has these capabilities on a low risk application may pose very little risk to C&G). In those exceptional scenarios, a broader definition to determine a privileged account must be considered.
Process	A series of actions, changes, or functions bringing about a specified set of outcomes. Processes may be broken down into procedures that represent role-based work instructions for those executing the processes.

Production	The production zone must host only those devices and servers that are under production control with appropriate business, functional and IT owners defined for them and are part of an operations run book for managing and configuring the device or server.
Public Information	Public information is information that can be disclosed to anyone or has been previously released into the public domain. Unauthorized disclosure, compromise, or destruction would not violate an individual's right to privacy, nor would such actions expose C&G to financial loss, embarrassment, or jeopardize the security of C&G assets. Information that is highly confidential, confidential or private information is defined as non-public information. (Refer to the Information Classification and Handling Standard for additional details).
Risk (corporate)	Risk is the possibility of exposure to business harm or loss. Corporate risk entails more than the commonly publicized vulnerabilities of Information Security such as viruses, worms, Trojans and hackers. It also includes operational, strategic, legal, regulatory compliance, credit, market, liquidity and branding (reputation) risks.
Risk Assessment	Risk assessment is an overall process to identify, analyze and prioritize risks.
Recovery Point Objective (RPO)	Describes the acceptable amount of data loss measured in time.
Recovery Time Objective (RTO)	Duration of time within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
Removable Media	Removable media are storage devices that can be removed from an information system. Examples of removable media include backup tapes, CDs, DVDs, Flash Drives, and USB drives.
Restricted Access Areas	Restricted Access Areas are facilities that require restricted access control because of special security program requirements. Examples of Restricted Access Areas may include: • Document retention rooms for critical records • Laboratories • Sensitive workgroups, including some R&D, IP, finance, or special project teams • Server rooms • Shipping and Receiving Areas • Training Rooms • Telecom and data communications areas (IDF/MDFs) • Data Centers
Restricted Information Systems	Restricted information systems include systems holding highly confidential information that is critical for C&G business. Examples include servers holding cardholder data, engineering lab servers/applications, etc.
Standard	Requirements that have been accepted as the practices against which results are measured. Standards must be incorporated into projects as Information Security requirements.
Software watermarking	Software watermarking is a technique to identify the ownership of a software code (or module). The process involves inserting a unique identifier to the software code.
Source Code	In computer science, source code is any collection of computer instructions (possibly with comments) written using some human-readable computer language, usually as text. The source code of a program is specially designed to facilitate the work of computer programmers, who specify the actions to be performed by a computer mostly by writing source code. The source code is automatically translated at some point to machine code that the computer can directly read and execute.

Suppliers	A supplier is a person or an organization that provides products or services to C&G . Suppliers can be either internal or external to C&G . Examples of suppliers include organizations and people who produce, distribute, or sell products, provide services, or publish information.
System Utility Program/Software	System utilities are software used to administer, configure, maintain or monitor an information system. Examples of system utilities include anti-virus software, backup software, patch management software, vulnerability scanning software, network utilities, system monitoring software, disk management software etc.
Technology (IT) Resources	IT assets which processes or stores information or data and is owned or licensed for use by C&G . These may be assets required to be used for and complete a set of specific activities.
Technical Configuration Standards and/or Guidelines	Recommendations or additional procedures that have been created for the user community to meet the security requirements defined in the Information Security Policy and Standards.
Technical Compliance Inspections	Technical compliance inspections can be defined as testing and/or examinations performed by organizations to verify compliance with their information security policy. This includes configuration reviews, penetration testing, vulnerability testing and other types of security testing. Testing is the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors. Examination is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
Threat	A potential for violation of Information Security, which exists when there is a circumstance, capability, action, or event that could breach Information Security and cause harm.
Tokenization	Tokenization is the process by which the primary account number (PAN) is replaced with a surrogate value called a "token". De-tokenization is the reverse process of redeeming a token for its associated PAN value. The security of an individual token relies predominantly on the infeasibility of determining the original PAN knowing only the surrogate value.
Users (also referred as C&G users)	Authorized C&G users include employees, contractors/consultants, service providers, contingent workers, interns, business partners, and vendors.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Acronyms

CMDB	Configurations Management Database
CRA	Corporate Risk Assurance / Internal Audit
CSA	Cloud Security Alliance
CSO	Chief Security Officer
CSS	Corporate Security and Safety
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention

GFM	Global Facilities Management
GPRS	General Packet Radio Service
GRC	Governance, Risk and Compliance
GSM	Global System for Communication
ISO	Information Security Office
IDS/IPS	Intrusion Prevention System/Intrusion Detection System
IPsec	Internet Protocol Security
IT	Information Technology
ISSA	Information Systems Security Association
ISO	International Organization for Standardization
OWASP	Open Web Application Security Project
PCI-DSS	Payment Card Industry – Data Security Standard
PMO	Project Management Office
PPO	Privacy Program Office
SANS	SysAdmin, Audit, Networking, and Security
SIO	Security Intelligence Operations
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP/WPA	Wireless Equivalent Privacy/Wi-Fi Protected Access

References

Referenced Item	Item Type and Description
British Standard (BS) International Organization for Standardization (ISO)/International Electro technical Commission (IEC) 27001:2013 – *Information technology – Security techniques – Information security management systems – Requirements*	This document serves as a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).
BS ISO/IEC 27002: 2013 Information technology – Security techniques – Code of practice for Information Security management	This document establishes guidelines and general principles for initiating, implementing, maintaining, and improving Information Security management in an organization.
NIST SP 800-53, Rev. 3: *Recommended Security Controls for Federal Information Systems and Organizations*	This document provides guidelines for selecting and specifying security controls for information systems.
Payment Card Industry (PCI) Data Security Standard (DSS), Version 2.0: *Requirements and Security Assessment Procedures*, October 2010	This document provides a baseline of technical and operational requirements designed to protect cardholder data.