

Citigroup Information Security Standards

Version 4.0: These standards are effective 8 April 2007. Compliance to these standards is in accordance with the "CISS 4.0 Compliance Requirements" document.

Purpose	3
Scope.....	3
Compliance	3
Non-Compliance	4
Owner	4
Format	4
Intranet Location	4
Standards	5
1. Information Ownership	5
2. Identification and Authentication	5
3. Authorization and Access Control	7
4. Confidentiality and Integrity	12
5. Incident Detection and Response	14
6. Information Security Administration	15
7. Training and Awareness.....	15
8. Vulnerability Assessments	16
9. Cryptography and PKI	16
10. Firewalls and Network Security Systems.....	17
11. Audit Logging	18
12. Developer Access to Controlled Information Systems (DAP).....	18
13. End User Computing (EUC).....	19
Definitions	20
Appendix A: Citigroup Cryptographic Requirements	27
Appendix A.1: Data Confidentiality Requirements	28
Appendix B: Schedule of Associated Documents:	30
Appendix C: Schedule of ISTG-Approved Technology:.....	32
Appendix D: CISS Standard Statement to ISO17799 Control Statement Mapping	33

Purpose

Compliance with the Citigroup Information Technology Management Policy (CITMP) Information Security Policy and these Standards (ISP&S) constitutes sound business practice and will assist Citigroup businesses in protecting information assets. These Standards represent the minimum requirements for information security that all businesses within Citigroup must follow. In addition, businesses may be required to incorporate information security practices and procedures as part of their compliance with other Citigroup policies.

Each business should document and maintain its security practices, procedures, and business requirements in compliance with the ISP&S.

Information Security is a business risk management issue. When determining the appropriate level of controls to safeguard Citigroup Information, the business, with the assistance of the Information Security Officer (ISO), must determine the Risk Level, the highest likely level of threat against the information, and ensure that suitable protection mechanisms are in place to avert and detect attacks resulting from these threats. The appropriate level of control depends not only on the risk to Citigroup, but also on the environment in which the information is stored, processed or transmitted. These Standards define categories for Information Classifications. Businesses can identify their information protection requirements based on these classifications.

To effectively secure Citigroup Information, Businesses must address the following fundamental questions:

- Do we know who is using the service?
- Can we control what they do and ensure confidentiality?
- Can we ensure the integrity of the information?
- Can we prevent unauthorized changes to information?
- Can we provide for non-repudiation of a transaction? (Can it be proved that someone performed a transaction?)
- Do we know:
 - If there is a problem?
 - Soon enough to take appropriate action?
 - How to minimize and contain the problem?
- Can we ensure the availability of information?

The Citigroup ISP&S will help Businesses answer these questions and provide the basis for an effective information security program.

If local laws or regulations establish a higher standard than provided here, Citigroup Businesses must comply with those laws. If local laws or regulations appear to conflict with these standards, the affected Citigroup business must consult with its local and regional compliance officers.

Scope

These Standards apply to Citigroup, its subsidiaries, and its managed affiliates worldwide.

Compliance

The Citigroup Information Security Standards (CISS) specify the results that must be attained, while each organization's applicable Processes and business-level procedures define how an organization will comply.

Each business shall ensure that its employees and Third Parties comply with the applicable sections of the CISS, and the business's information security practices and procedures.

It is the responsibility of each organization's Business Manager to ensure compliance with the Policy. Compliance means that an organization has implemented Processes and procedures that meet the requirements of the CISS and are appropriate to the level of risk.

Note: the term "Risk Level" is used throughout this document. Businesses may continue to use "Criticality" in lieu of "Risk Level" in determining the requirements applicable to a specific system.

The Audit and Risk Review organization audits operational integrity and for compliance with the CISS.

Non-Compliance

Non-compliance with the CISS by a Business or Technology organization must be documented, using a Global Operations & Technology Council (GOTC) approved form and Process. The completed form must indicate the reason for the non-compliance, compensating controls, and the related residual risks, and must be approved by both the business and the security management within the sector. Each GOTC member shall designate the appropriate business and security officers within their sector who must approve all such completed forms. Designation may be by name, title, or organizational role. The Information Security (IS) utility head for the sector is responsible for ensuring that the proper individuals have approved the form. The completed form must be sent to Information Security Services (ISS) and is effective when received by ISS.

ISS shall review non-compliance issues for both form completeness and the risk they present to Citigroup. If the risk is deemed excessive, ISS will escalate to the IS utility head and, if unresolved, to the GOTC member for that sector. Form completeness issues will be resolved with the IS utility head.

Owner

The owner of these standards is the Chief Information Security Officer (CISO). Questions / issues arising from the interpretation of these standards should be addressed to the Information Security Technology Group (ISTG).

Format

Unless specified otherwise within the text, numbered items are mandatory (should be read as "ands") whereas bulleted items are selections (should be read as "ors").

Throughout the Standards reference is made to various bodies with responsibility for aspects of the Standards, such as GOTC and ISTG. If from time-to-time between updates, the names or responsibilities of these bodies change or new bodies are created to assume some or all of their responsibilities, a notice will be placed on the CISS intranet location.

We are planning to move to the ISO17799 format in 2007. [Appendix D](#) maps CISS 4.0 to this ISO standard.

Intranet Location

The CISS and forms can be found on the Citigroup Intranet at <http://www.citigroup.net/informationsecurityservices>.

Standards

1. Information Ownership

- 1.1 Businesses will designate Information Owners, in writing, for Citigroup Information under their control.
- 1.2 The Information Owner will classify Citigroup Information under their control as one of the following Information Classifications:
 - RESTRICTED
 - CONFIDENTIAL
 - INTERNAL
 - PUBLIC
- 1.3 Each Business will follow the information security risk management Process and forms specified by GOTC.
- 1.4 Based upon the assessment Process and the classification of information, the Business will specify the level of security required to protect this information and ensure that sufficient controls are in place to achieve the specified level.
- 1.5 Each Business will ensure that an Inventory is maintained of Information Systems and Processes under their control and that it is maintained periodically as required. Additionally, each Business must review the Inventory at least annually for both accuracy and completeness. The Inventory will specifically identify the Information Owner, Information Classification and Risk Level .
- 1.6 Management must ensure that Information Systems are segregated on the Citigroup network in accordance with the following controls:
 - 1.6.1 Applications accessible to the Internet must be accessed via Demilitarized Zones.
 - 1.6.2 Citigroup hosts that permit access by Third Parties must have containment controls in accordance with [Citigroup 3rd Party Access Registry \(C3PAR\)](#) requirements.
 - 1.6.3 During an emergency event, Management must be able to filter access between portions of the network to reduce the impact from network Security Events (e.g. port filtering during a virus outbreak).
 - 1.6.4 Remote Access and Host Security must implement group based access controls (e.g. employees, vendors, customers) to limit access to network resources in the Citigroup network. At the host level, access control can be done at the group or individual level.
 - 1.6.5 Any network that fails to meet the requirements described in CISS sections 3.11.1; 4.6.2; 4.8.2; 6.5; or 10.1.1, or follow an approved exception process must be isolated from the Citigroup Network.
- 1.7 Network connections as the result of mergers or acquisitions must be firewalled until they have achieved "Trusted Network" Status as defined in the [ISTG-Approved Trusted Network Process](#).
- 1.8 Divestitures must follow the [Information Security Assessment Process for Mergers, Acquisitions, and Divestitures \(MAD\)](#) for network segmentation.
- 1.9 Servers supporting high risk applications must be located in facilities that meet the physical security requirements defined by [Citigroup Security and Investigation Services \(CSIS\) for "Data Centers" in the Global Security Policy](#).

2. Identification and Authentication

- 2.1 All Citigroup technology platforms will authenticate the identity of Users or systems accessing these platforms prior to initiating a session or transaction unless the User is entitled only to read INTERNAL or PUBLIC data on these platforms.
- 2.2 All Users will be:
 - 2.2.1 Uniquely identified or mapped to the technology platform by a User ID in accordance with the [ISTG-Approved Technical Requirements for Master IDs](#)
 - 2.2.2 Authenticated to the technology platform using a method of authentication commensurate with the risk associated with the Information System in accordance with the [ISTG-Approved Technical Requirements for Authentication](#)
 - 2.2.2.1 All use of shared authentication Infrastructure (e.g. Single Sign-on, Reduced Sign-on, and other shared authentication services) must be in accordance with the [ISTG-Approved Technical Requirements for Authentication](#).
- 2.3 Technology platforms will identify and authenticate peer technology platforms commensurate with the risk of the interaction and other mitigating controls. Where the risk has been otherwise mitigated, no additional authentication may be needed (e.g. If a system processes wire transfer instructions, then it must ensure that systems sending it those instructions are properly authenticated).
- 2.4 Users are accountable for all activity associated with their login IDs.
- 2.5 User static passwords will:
 - 2.5.1 Never be shared, made known to others or written down
 - 2.5.2 Never be displayed on the screen in clear text (with the exception of one time use).
- 2.6 Static passwords (other than PINs) will consist of a minimum of six (6) characters, which must contain both letters and numbers.
- 2.7 PINs may be used as the sole method of authentication to access Information Systems only if the PINs are:
 - Required by local laws or regulations or by rules adopted by self-regulatory bodies (e.g. central banks or payment associations with which Citigroup is associated)
 - Necessary to meet physical device constraints (e.g. keypad, telephone, smart card).
- 2.8 Login IDs associated with a static password must be disabled after not more than six (6) consecutive failed login attempts.
- 2.9 The Business will implement a documented Process to ensure that all static passwords are changed on a periodic basis and that login IDs are disabled after a stated period of inactivity. The periods selected will be commensurate with the level of risk of the Information Systems. The Business may waive the requirement for changing static passwords and disabling login IDs for customer access to Information Systems, provided that the Business periodically reminds its customers that manually changing their passwords provides greater security.
- 2.10 Networks must be protected from threats and security must be maintained for the Information Systems using the network. This includes information in transit across the network.
 - 2.10.1 Segregation of duties - Responsibility for Network Operations must be separated from responsibility for Computer Operations and in accordance with [CISS section 3.4](#).

- 2.10.2 Logging must be applied to enable recording and monitoring of network / Infrastructure security relevant actions in accordance with [ISTG-Approved Technical Requirements for Network Security Systems](#) and in accordance with [CISS section 11](#).
- 2.10.3 Externally facing Network De-militarized Zones (DMZs) must be managed as follows:
 - 2.10.3.1 Information with Information Classification of Confidential and higher must not be persistently stored on a system in an Internet facing DMZ. (See also [Appendix A.1](#)).
 - 2.10.3.2 DMZs and perimeter system operation must be implemented in accordance with [ISTG-Approved Citigroup Technical Standards for Perimeters](#).
- 2.10.4 External network connectivity that provides Third Party access to Citigroup resources requires management to ensure, either annually or when the Third Party status or access has changed, that the access accurately reflects the current status of the Third Party relationship.
 - 2.10.4.1 The Business requesting the Third Party network connection is responsible for maintaining the information regarding the Third Party relationship, including legal contracts, and communicating changes to the relationship to the Citigroup Infrastructure provider.
 - 2.10.4.2 Citigroup Infrastructure providers are responsible for maintaining information regarding the technical implementation of the connection and linking this to the relationship information provided by the Business responsible for the Third Party network connection.
 - 2.10.4.3 Citigroup Infrastructure providers must facilitate an entitlement review in accordance with [CISS section 3.4](#), including review of services, access permissions, and ownership.
- 2.11 Information Systems that use dynamic passwords or digital certificates will use [ISTG-Approved authentication services](#) to validate the credentials.
- 2.12 Functional IDs are exempt from (a) the restriction on sharing passwords, (b) the disabling of passwords after six (6) failed attempts, and (c) the periodic changing of passwords. Privileged functional accounts with Unix root, Windows Administrator, or other system administration access must have provisions in place to ensure individual accountability and are exempt only from (b).
 - 2.12.1 All Functional IDs must have a defined owner who is responsible for all aspects of the ID including usage, entitlement review, and password management. [Refer to the ISTG-Approved Technical Requirements for Functional IDs](#) for additional requirements.

3. Authorization and Access Control

- 3.1 Businesses will implement access controls that:
 - 3.1.1 Are fully documented
 - 3.1.2 Are auditable
 - 3.1.3 Ensure that Users are given only those privileges and entitlements necessary to perform their function.
- 3.2 Businesses will protect all Information Systems and Processes from unauthorized access and will secure them using security products, functions or Processes commensurate with the Risk Level of the Information Systems or Processes, and the Information Classification. This requirement

includes non-production environments such as unit acceptance testing, quality assurance and Development Systems.

- 3.2.1 Management must ensure that the use of Utility Programs that are capable of overriding system and application controls are restricted and controlled.
- 3.3 Access entitlements must be traceable to the Master ID, as defined in the [ISTG-Approved Technical Requirements for Master IDs](#), and the assigned owner.
- 3.4 Businesses must implement a documented Process to review and verify User entitlements to Citigroup's Information Systems.
 - 3.4.1 Businesses have responsibility for the end-to-end entitlement review Process around authorization and access control for all Users and Information Systems under their control. This includes ensuring reviews are performed for appropriate access and for notifying Information Security Administration (ISA) to remove unnecessary access.
 - 3.4.1.1 Businesses must ensure that duties are segregated for all Information Systems that they own (See Information Owner) to reduce opportunities for unauthorized access, modification, misuse, or denial of availability to the Businesses' assets. Segregation of duties must be implemented to prevent unauthorized or unnecessary disclosure in accordance with confidentiality and privacy requirements.
 - 3.4.1.2 Business managers may delegate entitlement reviews to individuals in their organization who have an understanding of the job functions / roles for those to be reviewed. Entitlement reviews for large organizations with common roles may also be delegated. Individuals may not review or approve either their own entitlements or the entitlements of an individual who delegated review responsibility to them.
 - 3.4.1.3 Businesses are responsible for ensuring that all Information Systems feed into a GOTC approved entitlement system.
 - 3.4.1.3.1 Until their systems feed into a GOTC approved entitlement system, the Business must ensure that their systems provide sufficient entitlement information for the appropriate ISA function to compile and distribute entitlement reports.
 - 3.4.1.3.2 The ISA function is responsible for providing entitlement reports to the appropriate Businesses for all Information Systems until they feed into a GOTC approved entitlement system.
 - 3.4.1.3.3 The Businesses must confirm receipt of the entitlement reports.
 - 3.4.2 In addition to entitlement reviews of Users, the following must be included in the Businesses' procedures where appropriate:
 - 3.4.2.1 Functional IDs: Functional ID owners must perform entitlement reviews in accordance with the [ISTG-Approved Technical Requirements for Functional IDs](#).
 - 3.4.2.1.1 A Functional ID owner may not be a user of any Functional ID owned by that individual.
 - 3.4.2.2 Entitlement Resource Owners: Entitlement Resource Owners are responsible for performing a review of any role / profile definitions associated with that resource on at least an annual basis.

- 3.4.2.3 Review Profile Owners: Review Profile Owners must, at a minimum, perform annual reviews of existing profiles.
- 3.4.3 Entitlement reviews must be completed for all Users semi-annually.
 - 3.4.3.1 All system entitlement reports (be they manually produced or automatically distributed through a user entitlement system) must include all of the following information:
 - User ID (login or access ID); User Name
 - Privileged access (e.g. SA, DBA, security administration, etc)
 - Master ID (GEID or RITS or SOE ID)
 - Department, P&L or other Business grouping identifier
 - Application / System ID (CSI)
 - Resource name (e.g. system name, database name, application name, etc.)
 - Resource type or description
 - Appropriate entitlement information related to the resource
 - Profile or group information (if available)
 - User ID creation date (if available)
 - 3.4.3.1.1 For high and medium risk applications, entitlement reports must also include Fine Grain Entitlements.
- 3.5 The Information Security Officer (ISO) is responsible for oversight of the entitlement review Process, providing support to enable the Businesses to complete entitlement reviews consistent with documented policies and procedures. The Business / Technology Manager will document and implement a Process to ensure access rights reflect changes in User status.
 - 3.5.1 Each Business / Technology Manager shall be responsible for the access rights of Users under their control. Required changes to existing access rights due to transfers and changes in job functions shall be formally communicated to the security administration function by the end of the next business day. The communication shall identify the access rights that need to be amended and the actual date when they are to be amended.
 - 3.5.2 For requests not related to User termination, access rights will be changed by the security administration function within 7 days of being notified of a change.
 - 3.5.3 Managers must notify security administration by the end of the next business day of User termination from Citigroup.
 - 3.5.3.1 The appropriate ISA function must execute User termination requests by, at a minimum, disabling User login (e.g. desktop / Active Directory, Single Sign-on, OTP tokens, remote access). The User termination must be completed by the end of the next business day.
- 3.6 A banner text, approved by the Legal Department for the Business, when supported by the operating system or application, must be displayed at all system entry points where a User initially signs on.
- 3.7 Remote access to Information Systems must be protected from unauthorized use.
- 3.8 Third Parties

- 3.8.1 Management will maintain appropriate security of Citigroup's information and Information Systems that are accessed, processed, or managed by Third Parties based on Risk Levels of the Information Assets. These risks must be identified and appropriate information security controls implemented in a reasonable time frame.
 - 3.8.1.1 Management must ensure that the security of their Information Systems are not compromised by the introduction of the products or services provided by a Third Party.
 - 3.8.1.2 Access to Citigroup's Information Assets and communication of information to Third Parties must be appropriately controlled based on Risk Level.
 - 3.8.1.3 Where appropriate, information security requirements ([CISS section 3.8.2](#)) must be addressed in a documented agreement with a Third Party following Processes established in [Citigroup's Vendor Selection and Management Policy & Standards](#).
 - 3.8.1.4 In accordance with the [ISTG-Approved Citigroup Application Vulnerability Assessment \(CAVA\) Process](#), new contracts with Third Parties which provide application services as part of the business relationship must include the right to periodically perform an independent Vulnerability Assessment. In addition, they must also include an obligation to remediate upon request, within the timeframes specified by the CAVA Process, any material issues found which lead to an Information System Vulnerability; and a right to terminate the contract on notice to the Third Party.
 - 3.8.1.5 Every Third Party relationship where the vendor has access to Citigroup information with a security classification of Confidential or higher must be evaluated annually to determine if a TPISA needs to be performed.
 - 3.8.1.6 Businesses must protect [Internal PII](#) when provided to Third Party vendors as required by local law.
 - 3.8.1.7 For new contracts, when access to Information with a security classification of Confidential or higher is given to Third Parties outside of Citigroup facilities and management oversight, the Business must perform a [Third Party Information Security Assessment \(TPISA\)](#) in accordance with the Operations Planning Group (OPG) approved TPISA Process.
 - 3.8.1.7.1 New contracts with a Third Party, where a TPISA was required to be performed, must include an obligation to have, upon request, any material issues found in the TPISA remediated. The contract must also include the right to terminate the contract, on notice to the Third Party, should the Third Party not remediate the issues in a timeframe specified by the TPISA Process.
 - 3.8.1.7.2 New contracts with Third Parties where the Third Parties is considered to be high risk, as determined by the [Information Security Risk Assessment \(ISRA\) Process](#) must have a TPISA completed and any material issues remediated or compensating controls established within two months of the signed contract.
 - 3.8.1.7.3 New contracts with Third Parties where the Third Parties is considered to be medium risk, as determined by the [Information Security Risk Assessment \(ISRA\) Process](#) must have a TPISA completed and any material issues remediated or compensating controls established within six months of the signed contract.

- 3.8.1.7.4 New contracts with Third Parties where the Third Parties is considered to be low risk, as determined by the [Information Security Risk Assessment \(ISRA\) Process](#) must have a TPISA completed and any material issues remediated or compensating controls established within 12 months of the signed contract.
- 3.8.2 Management must ensure that Third Party contracts involving access to high risk and Confidential Personally Identifiable Information (PII), as determined by the [Information Security Risk Assessment \(ISRA\) Process](#); or Restricted Information, adequately address the following information security requirements where appropriate:
 - 3.8.2.1 Protection of Citigroup Information Systems including:
 - 3.8.2.1.1 Protection against malicious software in accordance with [CISS section 4.6](#)
 - 3.8.2.1.2 Requirements that the Third Party notify the appropriate Citigroup Business when there has been any material compromise of Information Systems, or any unauthorized access or acquisition of PII, or as required by local legal or regulatory requirements
 - 3.8.2.1.2.1 Businesses must notify the appropriate BISO by the end of the next business day of receiving notification from the Third Party.
 - 3.8.2.1.3 Requirements that the Third Party returns or destroys customer information at an agreed point in time during or at the end of the agreement
 - 3.8.2.2 Access controls covering:
 - 3.8.2.2.1 The right of Citigroup to revoke access or to interrupt the connection between Citigroup and Third Party systems
 - 3.8.2.2.2 Notification to Citigroup of the identity of a subcontractor by the Third Party; the right of Citigroup to approve the subcontractor or a right to terminate the contract with notice to the Third Party
 - 3.8.2.2.3 If the security requirements of Citigroup change and the Third Party does not agree to such change, a right to terminate the contract with notice to the Third Party
- 3.8.3 If during a legal review, it is determined that a Third Party contract must include a requirement for a Third Party to notify the appropriate Citigroup Business when there has been any material compromise of Information Systems or any unauthorized access or acquisition of PII, then such provisions must be included in the contract.
- 3.9 Confidential and Restricted information must be stored on:
 - Citigroup managed devices
 - Third Party managed devices that are subject to a contract between the Third Party and Citigroup that contains confidentiality provisions consistent with Citigroup policies and standards
 - Devices owned by employees, contractors, and contingent employees when a GOTC member for the Business or (designee) approves, and the approval is documented.
- 3.10 If a Business permits individuals to access the Citigroup global network remotely, the Business must communicate to each individual that access must be conducted only over [ISTG-Approved remote access systems](#).

- 3.11 Businesses shall take appropriate steps, including technical solutions if available, as well as a having a periodic employee information security awareness program, to ensure its employees are aware of and understand that:
 - 3.11.1 Only [ISTG-Approved wireless local area networks \(WLANs\)](#) or other [ISTG-Approved wireless device solutions](#) may be connected to networks that contain Citigroup Information
 - 3.11.2 Employees are not permitted to access external Internet e-mail accounts from the Citigroup global network for non-business purposes
 - 3.11.3 Only [ISTG-Approved solutions for instant messaging, peer-to-peer networks or other Internet collaborative tools](#) are used to transmit or store Citigroup Information outside the Citigroup global network
 - 3.11.4 The use of remote access to the Citigroup global network (over wireless, broadband, dialup, etc) is not permitted unless the remote connection is made through an [ISTG-Approved virtual private network \(VPN\)](#) or [ISTG-Approved remote access web portal](#)
 - 3.11.5 Except as set forth in [CISS section 3.10](#) above, only Public and Internal Information may be stored on employee owned devices (e.g. home computers, personal digital assistants, mobile Internet and e-mail appliances).
- 3.12 Only Citigroup owned and managed devices or vendor devices that comply with these Standards and are supervised and authorized by the Business may have direct access to the Citigroup global network.

4. Confidentiality and Integrity

- 4.1 Businesses will inform employees, agents, contingent workers and contractors who use Information Systems or Processes (in particular e-mail, voice mail and computer systems) that all information stored, transmitted or handled by these systems or Processes is the property of Citigroup, its customers or licensors, and, where permitted by local law, this information may be reviewed and monitored for administrative, security and other lawful purposes. Citigroup reserves the right, as permitted by law, to obtain information, including Worker information, from all of its systems and Processes for administrative, security, and other lawful purposes.
 - 4.1.1 Management must ensure that [Citigroup's Electronic Communication Policy on Acceptable Use](#) has been communicated to all employees, agents, contingent employees, contractors and Third Parties working at Citigroup facilities.
- 4.2 Businesses will protect Citigroup Information regardless of the media upon which it is maintained. This Standard applies, but is not limited to, the following types of media upon which information is contained, recorded or stored: cards, cassette, CD, check stock, diskette or other removable storage devices, hard copy output, magnetic disk, magnetic tape, microfilm, microfiche, optical disk or paper documents.
- 4.3 [Appendix A.1](#) specifies the types of information and under what conditions information must be encrypted or otherwise cryptographically protected. If a cryptographic protection mechanism is not required, the Business must still protect Citigroup Information from unauthorized access, modification, or deletion.
 - 4.3.1 Information placed upon electronic transportable media must follow additional requirements as defined in the GOTC approved [Electronic Transportable Media \(ETM\) Standard](#).

- 4.4 Each Business unit will develop, document and enforce a secure workspace program that protects all RESTRICTED and CONFIDENTIAL information stored on any media from unauthorized access.
- 4.5 RESTRICTED and CONFIDENTIAL information at the point at which the information is no longer useful to the Business plus any additional period of retention required by law, regulation or contract will be destroyed in a manner commensurate with the Information Classification of the information.
- 4.6 Management must ensure that precautions are taken to prevent and detect the introduction of malicious code (e.g. viruses, Trojan-Horse, spyware) and must implement preventive, detective, and recovery controls to protect against malicious code. Management must:
 - 4.6.1 Provide Users with appropriate awareness training regarding malicious code
 - 4.6.2 Implement, update, and maintain [ISTG-Approved technology for anti-virus and anti-spyware](#) on all personal computers and [ISTG-Approved technology for anti-virus](#) on all local area network (LAN) servers, mail servers and other devices that store content received from external sources (provided that an ISTG-Approved technology is available for the device)
 - 4.6.3 Establish an appropriate blocking strategy on the network perimeter
 - 4.6.4 Implement technical and Process controls to ensure that employees do not access external Internet e-mail accounts from the Citigroup global network for non-business purposes
 - 4.6.5 Implement perimeter Infrastructure that provides the capability for blocking access to Internet sites that are deemed to be non-business related or present an information security risk.
- 4.7 Management must ensure that precautions are taken to appropriately control the use of Mobile Code. Where the use of Mobile Code is authorized, the configuration must ensure that the authorized Mobile Code operates according to a clearly defined security policy, and unauthorized Mobile Code must be prevented from executing.
 - 4.7.1 For Mobile Code that can affect the underlying operating system or platform (i.e. outside the 'sandbox') management must ensure the following:
 - 4.7.1.1 Mobile Code published by Citigroup must be signed using a certificate from an [ISTG-Approved Certificate Authority](#)
 - 4.7.1.2 Mobile Code published by Third Parties must be signed by an [ISTG-Approved Certificate Authority](#)
 - 4.7.1.3 Resource owners must implement a Process that ensures that a valid Certificate Authority signs the Mobile Code and that the lifecycle of the certificate is managed to address expiration or rotation of the certificate
 - 4.7.1.4 Signed Mobile Code with expired certificates must be removed from production.
- 4.8 Management must ensure that:
 - 4.8.1 Only operating systems and software that are currently supported by an approved vendor or have an active and appropriate release of patches and configuration updates available to address security issues are used

- 4.8.2 All approved security patches and configurations are applied within the time periods specified by the [ISTG-Approved Vulnerability Threat Management Process](#)
- 4.8.3 New vendor contracts for software products or services (off the shelf or custom) include remediation timeframes for Vulnerabilities in the vendor's software.
- 4.9 Each Business must ensure that Third Parties (excluding customers accessing their own information) properly handle and protect Citigroup Information to which they have access.
- 4.9.1 Each Business shall ensure that Third Parties that store, process, manage or access Citigroup Information (except Internal and Public Information) or have connectivity to Citigroup's network resources comply with the applicable sections of the CISS or provide equivalent controls.

5. Incident Detection and Response

- 5.1 Management will ensure an effective approach is applied to the management of information security incidents and comply with the [Citigroup Security Incident Response Team \(SIRT\) Process](#).
 - 5.1.1 The following IS incidents, events and Vulnerabilities must be reported as follows:
 - 5.1.1.1 Suspected viruses and / or malicious code must be reported immediately to an individual's or group's designated help desk or support structure.
 - 5.1.1.1.1 Confirmed Trojan-Horse viruses must be treated as IS incidents.
 - 5.1.1.1.2 Viruses that cause a denial of service and / or are specifically targeted at Citigroup must be treated as IS incidents.
 - 5.1.1.1.3 Viruses that appear to affect multiple machines must be reported to Citigroup Threat Assessment Center (CTAC) (<http://www.citigroup.net/ti/ctac>).
 - 5.1.1.2 For Third Party incidents, management must follow the Third Party requirements for event and incident reporting in accordance with [CISS section 3.8.2.1.2](#).
 - 5.1.1.3 Application Vulnerabilities must be reported to the ISO responsible for the application.
 - 5.1.1.4 Infrastructure Vulnerabilities must be reported to the Vulnerability Threat Management (VTM) team (http://www.citigroup.net/informationsecurityservices/pdf/vtm_teams.pdf).
 - 5.1.1.4.1 The VTM team must maintain a Process to gather, collect, analyze, and disseminate Infrastructure Vulnerabilities from external sources.
 - 5.1.1.4.2 The VTM team must maintain a Process to gather, collect, analyze, and disseminate threat information from external sources.
 - 5.1.1.5 Suspected phishing events may be reported to submitphishing@citigroup.com.
- 5.2 Customer facing organizations must have and must communicate a Process to their customers to report security related events.
 - 5.2.1 Based on Risk Level, management must train customer facing service personnel to identify and report customer calls that may be the result of IS events. At a minimum, awareness materials covering security incidents must be given to all customer facing service personnel.

- 5.3 Management must have a Process to ensure that Infrastructure Vulnerabilities that result in a compromise of Citigroup's Information Assets are reported to the ISO supporting the Process owner.

- 5.3.1 All testing or verification of Vulnerabilities must only be conducted by personnel authorized by the VTM or SIRT Team or as part of an authorized audit activity.

- 5.3.1.1 Other Users that discover Vulnerabilities must not attempt to independently validate the Vulnerability.

6. Information Security Administration

- 6.1 Businesses will ensure that appropriate background and reference checks are performed on all Citigroup staff (that is, job applicants who have accepted a job offer and Third Parties) who perform security-related functions or who are granted highly privileged access (e.g. system administration, database administration, change control or supervisor status) to Citigroup Information.
- 6.2 Each Business will incorporate information security procedures into their Processes and procedures for the selection, development and implementation of applications, products and services in order to ensure compliance with these Standards.
- 6.3 Any individual assigned to the role of ISA must not perform transactions that conflict with this role. Specifically, they must not initiate, program, Process or authorize business transactions.
- 6.4 Commensurate with the Risk Level of the Information Systems:
 - 6.4.1 Systems administration and security administration functions must be segregated to provide separation of duties for the same system.
 - 6.4.2 Administrative actions (e.g. adding / deleting users, changes to entitlements / passwords or system security configurations) require an independent verification or maker / checker Process.
- 6.5 The ISA function for systems owned and managed by Citigroup must not be outsourced unless approved by the Business head and their GOTC representative.
 - 6.5.1 If outsourced, a documented Process must be implemented to manage Third Party activity in compliance with Citigroup policies and standards.
- 6.6 Each Business will implement a Process to ensure that all security functions, products, tools and services are configured to meet these Standards and that all default access capabilities are removed, disabled or protected to prevent their unauthorized use.
- 6.7 All information security management functions that are relocated across country borders must have documented approval of the appropriate GOTC member that owns the application or their designee.
- 6.8 At least annually, each Business must:
 - 6.8.1 Review its information security practices and procedures for compliance with the [Information Security section of the CITMP](#) and these Standards. The review will assess the adequacy of these practices and procedures based on changes in their Processes, technology, business responsibilities, the sensitivity of Citigroup customer or corporate information and the risks that may threaten this information.

7. Training and Awareness

- 7.1 Each Business shall ensure that all employees, contractors, contingent workers, agents, temporary staff and anyone who is new to Citigroup or who has had a significant change in job responsibility, receive training on the information security related aspects of their job function within 90 days of the job commencement.
- 7.2 Each Business shall ensure that all employees, contractors, contingent workers, agents and temporary staff who are:
 - 7.2.1 Web software Developers or information security officers complete annually a GOTC-approved information security training program specific to their function.
 - 7.2.2 Systems administrators and security administrators, who manage or support Citigroup Information Systems, receive a GOTC approved training course at least every 36 months.
- 7.3 Each Business shall ensure that all employees, contractors, contingent workers, agents and temporary staff:
 - 7.3.1 Annually receive GOTC-approved awareness material on (i) information security and (ii) the information security aspects of their job function.

8. Vulnerability Assessments

- 8.1 All Businesses will ensure that all Citigroup products, services or applications:
 - 8.1.1 Implement the [ISTG-Approved Citigroup Application Vulnerability Assessment Process](#)
 - 8.1.2 Undergo an Application Vulnerability Assessment as described in the [ISTG-Approved Citigroup Application Vulnerability Assessment Process](#).
- 8.2 Managers of technology Infrastructures will ensure that annual Vulnerability Assessments of their technical Infrastructure are performed in accordance with the [ISTG-Approved Citigroup Infrastructure Vulnerability Assessment Process](#).
- 8.3 High-risk findings identified in the Vulnerability Assessment will be resolved before the product, service or application can go live or updates introduced into the production environment. The application or systems manager will maintain a record of all actions taken to resolve the high-risk findings.

9. Cryptography and PKI

- 9.1 Management must ensure adequate controls are in place for each of the following key management Processes:
 - Generation
 - Distribution
 - Storage
 - Renewal
 - Revocation
 - Recovery & Escrow
- 9.1.1 Key management must follow the [ISTG-Approved Technical Requirements for Cryptography](#).
- 9.1.2 [ISTG-Approved cryptographic algorithms](#) and minimum key lengths must be used to implement encryption.
- 9.1.3 Digital certificates used by the application must be issued by [ISTG-Approved certificate providers](#).

- 9.1.4 Wireless networks must be encrypted with [ISTG-Approved encryption algorithms](#).
- 9.2 Businesses utilizing any form of cryptographic mechanism must use [ISTG-Approved key management tools and techniques](#).
- 9.2.1 The ISTG must consider applicable legal and regulatory requirements in the relevant jurisdictions when approving cryptographic mechanisms.

10. Firewalls and Network Security Systems

- 10.1 Businesses responsible for managing or maintaining internal Citigroup networks will ensure that:
 - 10.1.1 All external IP connections to the Citigroup global network are protected by a Citigroup managed firewall.
 - 10.1.2 All external IP connections to the Citigroup global network are monitored by a real-time intrusion detection system (IDS) or intrusion prevention system (IPS).
 - 10.1.3 Non-Internet connections for Third Parties (e.g. B2B) to the Citigroup network are monitored by a network based anomaly detection (NBAD) system or Intrusion Detection or Prevention System (IDS / IPS).
 - 10.1.4 For shared networks, especially those extending across the organization's boundaries, the capability of Users to connect to the network must be restricted, in line with the access control policy and requirements of the business applications (e.g. locations to where we extend Citigroup Infrastructure that is not our own facility, but where we maintain the resources in that location).
 - 10.1.4.1 Network connectivity must be as limited as possible and follow [ISTG-Approved Technical Requirements for Perimeters](#).
- 10.2 Only [ISTG-Approved Network Security Systems](#) (firewalls, intrusion detection systems, intrusion prevention systems, and network based anomaly detection system) and Security Service Providers may be used.
 - 10.2.1 External firewalls must be configured with a default "deny all" rule.
- 10.3 All configuration changes to firewalls and IDS / IPS / NBAD systems must be implemented through approved [CITMP change control mechanisms](#).
- 10.4 When a suspicious Security Events occurs, a SIRT response must be generated and escalated through the defined [SIRT Process](#) and procedure.
- 10.5 Network connectivity between Citigroup and Third Parties must follow [ISTG Approved Technical Standards for Inter-Corporation Connectivity](#).
 - 10.5.1 Using the Citigroup network to connect a Third Party to another Third Party where Citigroup provides no intermediary business services is prohibited.
- 10.6 All system alarms associated with a firewall or IDS / IPS / NBAD generated Security Event must be logged and archived daily and reviewed for Security Events.
- 10.7 Management must demonstrate the ability to respond to a Security Event within 15 minutes of the occurrence on a 24-hour by 7 days per week basis. This includes but is not limited to alerts generated from IDS / IPS / NBAD.
- 10.8 Each Business and Technology Manager shall ensure that all IP connections to Third Parties are protected by CTI-managed firewalls. Business and Technology Managers are responsible for ensuring compliance with this requirement throughout any change of status in a Third Party (e.g., an acquisition or divestiture).

11. Audit Logging

11.1 Businesses will ensure that all Information Systems that process or store Citigroup Information use audit trails to log and report:

11.1.1 All attempted violations of system security. E.g.:

- Failed User login attempts
- Invalid User attempts to access sensitive entitlement resources

11.1.2 All significant events relating to security and system administration, system operator changes, financial transactions and customer information must be logged.

The level of audit trail reporting shall be commensurate with the Risk Level of the Information Systems.

11.1.2.1 Significant events, such as financial transactions or changes to Confidential PII must be captured if the system is high or medium risk.

11.1.2.2 Significant events such as changes done by the ISA function (e.g. user creation, modification of User access rights, deletion, creation and modification of roles / profiles on the application, password reset, changes to system security configuration) must be captured. Query and view activities are out of scope.

11.1.3 Application and system owners must ensure that access controls are in place to preserve the integrity of audit trails in storage and during transmission.

11.1.4 Audit trails must be retained in accordance with [Citigroup Records Management Policy- ISY160](#).

11.1.5 The clocks of all relevant information processing systems within an organization or security domain must be synchronized with an agreed accurate time source.

11.2 Businesses will ensure that a maker / checker Process exists or audit trails are reviewed on a periodic basis commensurate with the risk of the Information Systems.

11.2.1 Any suspicious activity must be acted upon immediately.

11.2.2 The review Process must be segregated to ensure the reviewers do not review their own activity.

12. Developer Access to Controlled Information Systems (DAP)

12.1 General Access Policy

12.1.1 A Developer must not be granted access to any Controlled Information System except on a temporary basis. See CISS sections 12.1.2 and 12.1.3, below.

12.1.2 A Developer must not promote, move or copy code or data to or from a Controlled Information System.

12.1.3 A Developer must not be granted the ability to modify code or data on a Controlled Information System.

12.2 Emergency Access Policy

- 12.2.1 Emergency access to a Controlled Information System may be granted to a Developer on an event-by-event basis for application problems. This access must be authorized and controlled in accordance with [ISTG-Approved Technical Requirements for Developer Access to Controlled Information Systems](#).

12.3 Sensitive Data on Non-Production Systems

- 12.3.1 It is not permitted to put Sensitive Data on a Non-Production System unless the following requirements are met:
 - 12.3.1.1 Before any Production Data can be moved or copied to a Non-Production System ("target"), the Application Manager, in conjunction with the Information Owner, must identify and document all data items in the "source" Controlled Information Systems that contain Sensitive Data.
 - 12.3.1.2 The copying to or from, and the use of Sensitive Data on a Non-Production Information System must be approved by the ISO and Information Owner as part of a documented approval Process.
 - 12.3.1.3 Once all Sensitive Data items have been identified and documented and the migration / use approved, Sensitive Data may only be moved or copied to the target if:
 - 12.3.1.3.1 The data has been irreversibly Redacted so it is no longer sensitive using ISTG-Approved tools / methods, or
 - 12.3.1.3.2 The Non-Production System is subject to the same controls as the production system.

- 12.4 All Developer access to Controlled Information Systems must be in accordance with [ISTG-Approved Technical Requirements for Developer Access to Controlled Information Systems](#).

13. End User Computing (EUC)

- 13.1 IT controls over End User Computing are evaluated through the business [Risk and Control Self Assessment \(RCSA\) Process](#). This risk management program defines the subset of all EUCs that are considered "critical" as determined by the End User Computing Controls Appendix to the RCSA Policy.
 - 13.1.1 "Critical" EUCs must be included in the [Information Security Risk Assessment \(ISRA\)](#) review.
 - 13.1.2 "Critical" EUCs must undergo a review of IS and IT controls, as outlined in the RCSA appendix.
 - 13.1.3 No IS non-compliance assessment is required for EUCs, as relevant risks are captured in the business risk assessment program.
 - 13.1.4 Note that there is no other IS Inventory requirement (including CSI) for EUC other than inclusion in ISRA.

Definitions

Application Manager	An Application Manager is typically the Technology Manager or Business manager; and, in the case of Third Party-developed applications, is directly responsible for the development, maintenance, configuration, or functional specifications of the application.
Authentication Data	Passwords, PINs, private cryptographic keys, shared keys, one time use, dynamic or pre-expired passwords.
Business	This term applies to multiple levels of the organization such as a Citigroup line of Business (e.g. an industry, product, market or geographic segment) or a functional unit (e.g. O&T, HR, Legal, Risk Management, Finance, Corporate Center). The term “Business managers” may be interpreted as Business or Technology Managers, depending on whether the function is of a business or technical nature.
Citigroup Information	All transactional records, customer information, memos, reports, e-mail, software and other data created by Workers and Third Parties during the course of business or otherwise owned or managed by Citigroup.
Citigroup Infrastructure	The premises, physical hardware, technology components or collection of components that store, process or transmit Citigroup Information. This includes operating systems, management utilities, and core software and the associated Processes required to manage these locations, devices or software as determined by the Business.
Coarse Grain Entitlements for Employee Entitlement Review System (EERS)	Entitlement information that include only the login to the application.
Computer Operations	The management of servers, workstations, operating systems, system applications and databases in accordance with Business requirements. Activities include management of uptime and performance, management of identity and access, management of configurations, and management of patches and the safeguarding of the confidentiality and integrity of data resident on these systems.
Controlled Information System	A Controlled Information System is defined as a production, Continuity of Business (CoB) or UAT application, database, operating system or device containing Production Data. For purposes of persistent Developer read access only, a Controlled Information System is defined as a production, Continuity of Business (CoB) or UAT application, database, operating system or device containing Production Data with an Information Classification of Confidential (Confidential in this case

	includes Confidential PII or Sox 404 related financial information only) or higher.
Criticality	The impact (High, Medium or Low) to the Business if Citigroup Information is subject to a loss of integrity, confidentiality or availability determined as a result of the risk assessment Process.
Demilitarized Zone (DMZ)	A buffer zone between a "hostile" network, such as the Internet, and a "trusted" network, such as the corporate LAN. The buffer zone contains systems specifically hardened for that environment and mandatory access control between the hostile network and the buffer, and the buffer and the trusted network.
Developer	A Developer is anyone responsible for the programming of end-user applications. Programming refers to the writing or changing of source code, stored procedures, or scripts that create or change the functionality of the end-user application. The term Developer can refer to a specialist in one area of computer programming or to a generalist who writes code or customizes functions or scripts for many kinds of software.
Development System	A system used by Developers to create, modify and test code.
EERS Profile	Any grouping of entitlements (Coarse or Fine Grain, application, or resource, etc). Profiles can be defined for a physical set of assets (e.g. RACF groups, Unix groups, Top Secret profiles) or a logical set of assets (e.g. Citigroup eLabels).
Entitlement Resource Owner	A designated owner of a resource that requires user identification / login. A resource can be an application, system, database, product, Third Party application, service, or other type of Information Asset.
Fine Grain Entitlements for Employee Entitlement Review System (EERS)	Entitlement information that provides a further breakdown of specific functions or actions that each User can invoke.
Functional IDs	Generic accounts (e.g. Root, Administrator) that are required by the operating system, system level software or utilized by automated Processes and are associated with a group, function or role.
GOTC	GOTC (the Global Operations & Technology Council) is chaired by the Chief Operations and Technology Officer and is composed of the Chief Technology Officer from each Business or sector. GOTC reviews adjustments to the IS program that require Board approval, such as the information security strategic direction and appropriate policies and standards; it oversees the implementation of IS Program elements; ensures consistent company-wide implementation of management metrics and reporting systems, Processes and responsibilities to accurately measure and report the Business' IS risks, security incidents, IS Program's status and performance; and ensures that sufficient and appropriate resources are available to address the requirements of the IS Program. GOTC

	members are accountable for the success of the IS Program within their Business or sector.
Information Assets	Information Assets are physical and logical constructs that participate in the processing of information on behalf of Citigroup. E.g. laptops, blackberries, servers, desktops, applications, operating systems, , and network devices, .
Information Classification	Information Classification is critical in determining the controls required to protect the Information System or Process. Citigroup Infrastructure must always use the classification that it is intended to service. Where multiple classifications are present, then the highest level of classification must be selected. Citigroup Information is classified as follows: • RESTRICTED Information that, if disclosed to unauthorized individuals, could have a significant impact on Citigroup's legal or regulatory obligations or on its financial status, customers or franchise. • CONFIDENTIAL Information that Citigroup Businesses are obligated to protect including, but not limited to information belonging to: customers, Workers, Third Parties, or Citigroup Businesses. Any combination of data subject to regulatory or contractual restrictions on disclosure. Information that the Business determines has the potential to provide a competitive advantage or have a significant impact on the Business if disclosed to unauthorized individuals. The following Personally Identifiable Information (PII) is considered Confidential: • Any combination of PII that identifies an individual human being in a manner that would facilitate identity theft, credit fraud or other financial fraud. • Any PII that constitutes special information under applicable country law or regulation that requires encryption of such data. • Some examples of Confidential PII include, but are not limited to: a. Customer name or contact information in combination with social security number, national ID or tax number, drivers license, passport or account number

	b. Citigroup Worker name, Worker ID or contact information in combination with race, religion, ethnicity, citizenship, political affiliation, or union membership c. Citigroup Worker name or Worker ID in combination with employee performance appraisal, compensation information, or employee medical information. • INTERNAL Information that is commonly shared within Citigroup is not intended for distribution outside Citigroup and is not classified as RESTRICTED or CONFIDENTIAL. The following PII is considered Internal: • Information that enables internal Processes, such as communications, identification, or administration will be treated as Internal. Some examples of Internal PII include, but are not limited to: a. Citigroup Information that may contain Citigroup Worker names, Worker IDs and contact information b. Continuity of Business (CoB) call trees that may contain Citigroup Worker IDs and contact information, including personal contact information c. Citigroup Worker names, Worker IDs and contact information, or customer names and contact information when only used for Citigroup system to system communication. • PUBLIC Information that is freely available outside of Citigroup or is intended for public use by the Information Owner.
Information Owner	The manager that presides over a supported Business area and is the primary owner of the information that is stored or processed. Where the information is owned by multiple Businesses, the primary owner of the Information System or Process may be selected by various criteria such as largest dollar contributor, most number of users or highest financial firm-risk.
Information Systems	The products, applications, services, and Citigroup Infrastructure used to store, process or transmit Citigroup Information.
Infrastructure	The active technology components, facilities and human resources that form the underlying technology foundation, upon which business systems and technology support mechanisms operate. It is divided into three key components: • Technology Infrastructure (TI) - All network attached devices, their core operating systems, and basic user interface

	- Facilities Infrastructure (FI) - All tech rooms, wiring closets, server rooms, and raised floor data centers housing Technology Infrastructure - Human Resources Infrastructure (PI) - All personnel, and their management chain, whose primary job function is the engineering, system administration, security administration, or maintenance of Technology Infrastructure or Facilities Infrastructure.
Inventory	Listing or information base where all entries are uniquely identified by their description and particular characteristics. Inventories required as part of information security initiatives and programs are used to facilitate adherence to policies, standards and regulations. Each specific program or initiative will dictate the requirement, if any, for an Inventory as well as any details around the periodic review or updating of the Inventory.
ISTG-Approved Technical Requirements	The Information Security Technology Group (ISTG), document that describes the technical security requirements for a given information security Infrastructure product or Process.
Master ID	The Master ID is the Global Enterprise ID (GEID), as defined in the ISTG-Approved Technical Requirements for Master IDs .
Mobile Code	Applications or utilities that are downloaded dynamically, typically by web browsers, and stay resident on the end user system. Common examples include ActiveX controls and Java applets. This definition applies to items consumed by Citigroup Users or published by Citigroup applications.
Network Operations	The management of network Infrastructure, network perimeters and network equipment in accordance with Business requirements. Activities include management of identity and access, management of configurations, management of patches, safeguarding the confidentiality and integrity of data passing over the networks, optimizing the network performance and applying appropriate logging and monitoring.
Network Security Domains	Logical or physical constructs that create a level of controls for an environment that allow for the isolation of risks and issues from portions of the network or system that is outside of a given domain. This could be accomplished by a combination of network access controls like IPSec, port filtering, Access Control Lists (ACLs), and firewalls, virtualization, or host level controls like Logical Partitioning (LPAR) on Mainframes.
Non-Production System	A system used to test or otherwise emulate the production system. This includes, but is not limited to, systems classified as test, UAT or development. A CoB system can be considered non-production if it is

	being used as a test, UAT or Development System.
Persistent Storage	Persistence relating to storage refers to the ability to retain data structures between program executions, such as, for example, an image-editing program saving complex selections or a word processor saving undo history. This is achieved in practice by storing the data in non-volatile storage.
Personally Identifiable Information (PII)	PII is any information that identifies a human being. Some PII must be treated as Confidential (see definition of Confidential).while some may be treated as Internal (see definition of Internal).
PIN	Personal identification number that is a form of static password consisting only of numbers.
Process	All Business procedures (including manual procedures) that process Citigroup Information and perform a significant business function.
Production Data	Production data includes both the source code and application specific data, including data such as customer or employee information.
Profile Owner	A designated owner of a Profile. This may or may not be the same person as the Entitlement Resource Owner.
Redaction	Editing or cleansing of the data so the original content is no longer recognizable or reproducible; or, in the case of Confidential Personally Identifiable Information (PII), no longer identifiable to an individual.
Review Profile	A grouping of entitlements to a resource or resources which are typically assigned to a common job classification, role, or class, and then ONLY used to facilitate the entitlement review Process (e.g. Review Profile function in EERS.) The grouping of entitlements within a review profile must be reviewed at least annually by the Review Profile owner.
Risk Level	In this document, Risk Level refers to inherent risk. Risk Level is the product of the likelihood of an adverse event and the impact that threat could cause to the Business.
Security Event	A system / network / application alarm or series of alarms that may lead a security administrator or information security officer to believe a security incident has occurred, or is about to occur.
Security Service Providers	Organizations that perform security functions for applications or network Infrastructure. This includes, but is not limited to: monitoring of Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) and firewalls, information security administration, log reviews, Vulnerability scanning / assessments.
Sensitive Data	Authentication Data, or data classified as Confidential or higher, or where restricted by local laws and regulations.
Technology Manager ("TM")	A member of the Citigroup Information Technology Leadership Council (ITLC) or any other senior

	manager with responsibility for managing the Citigroup Infrastructure for one or more Businesses.
Third Party	Any entity that does not meet each of the following conditions: 1. Majority-owned or controlled by Citigroup; 2. Subject to Citigroup's policies and standards; 3. Subject to review by Audit and Risk Review (ARR) as an "auditable entity" and reported to the Audit Committee of Citigroup's Board of Directors; 4. Complies with and participates in Citigroup security Processes such as SIRT, and GEM.
User	Any employee, temporary worker, or Third Party (excluding customers) with access to Citigroup Information Systems.
Utility Program	A tool or application that is used to modify or view a system or application's data, structure, or configuration.
Vulnerability	A characteristic or condition (including a weakness) of an Information Asset or group of Information Assets which can be exploited by a threat.
Vulnerability Assessment	A Process to identify Vulnerabilities in applications or systems using such methods as ethical hacking, source code analysis, vulnerability scanning, etc.
Worker	Citigroup Worker means past and present employees, non-employees, directors, consultants, individual contractors, contingent workers, temporary workers, and job applicants of Citigroup Inc. and its affiliates, as well as their respective dependents, family members, domestic partners, emergency contacts and other individuals whose personal data are provided to Citigroup or its affiliates within the context of the working relationship.

Appendix A: Citigroup Cryptographic Requirements

The use of cryptographic mechanisms can be applied to any one or more of the following control requirements:

- Data Confidentiality
- Data Integrity
- Non-Repudiation

Appendix A.1: Data Confidentiality Requirements

In accordance with [CISS section 4.3](#), this Appendix A.1 provides additional requirements as to when Citigroup Information must be encrypted. The primary factor in determining whether Citigroup information must be encrypted is the Information Classification of the data. This determines the base encryption requirement, which is supplemented by criteria for certain specific environments.

The following table describes the base encryption requirements:

PUBLIC and INTERNAL Information	There is no requirement to encrypt this information.
CONFIDENTIAL Information	Confidential in transmission¹: - Confidential Information must be encrypted when transmitted outside of a Citigroup managed Infrastructure. - Confidential Information must be encrypted when transmitted within a non-Citigroup managed Infrastructure that does not meet Citigroup Security standards as demonstrated by a TPISA assessment as well as when a TPISA assessment has not been completed. Confidential being Persistently Stored: - Confidential Information does not have to be encrypted when stored in Citigroup managed Infrastructure. - Confidential Information must be encrypted when Persistently Stored in a non-Citigroup managed Infrastructure that does not meet Citigroup Security standards as demonstrated by a TPISA assessment as well as when a TPISA assessment has not been completed.
Confidential Personally Identifiable Information (PII) – a subset of CONFIDENTIAL Information	Confidential PII in transmission¹: Where legally allowed, Confidential Citigroup PII must be encrypted when sent over a non-Citigroup managed Infrastructure. Confidential PII being Persistently Stored: - Confidential PII does not have to be encrypted when stored in Citigroup managed Infrastructure. - Confidential PII must be encrypted when Persistently Stored in a non-Citigroup managed Infrastructure that does not meet Citigroup Security standards as demonstrated by a TPISA assessment as well as when a TPISA assessment has not been completed.
RESTRICTED Information	The base requirement is to encrypt Restricted Information when transmitted or Persistently Stored.
Authentication Data	Authentication Data, except one time use, dynamic or previously expired passwords, must be encrypted in all environments.

¹ The transmission of data can take many forms including, but not limited to Electronic File Transfers (e.g. FTP, NDM), Web Traffic, E-Mail, Inter-Process Communications (e.g. application to application) using various protocols, Tapes, and CDs / DVDs / Disks.

Any information, once encrypted in compliance with these standards, may be treated as PUBLIC when separated from the encryption key.

In addition to the base encryption requirement, additional criteria have been defined for the following environments:

- Databases – Restricted information stored in databases may be stored unencrypted so long as the controls defined by the [Database Security Guidelines](#) are met to control access to the database. This exclusion does not apply to Authentication Data (e.g. passwords) that must be encrypted.
- External Individual e-mail – Email may be sent or persistently stored unencrypted where:
 - (i) the email does not contain information with a security classification of Confidential PII, Restricted or Authentication data; or
 - (ii) where encryption is prohibited by local law or will inhibit a Business from complying with its legal or regulatory obligations; or
 - (iii) a technological solution has not been deployed to the Business by the Business's technology provider that enables / permits compliance with the encryption requirements contained in this document.
- Private networks that are independently regulated by a recognized authority and are considered a Financial Services Industry standard for transacting business between licensed or accredited counterparties (e.g. SWIFT or Central Bank) may be considered exempt from the Confidential PII in transit encryption requirement until such time that those networks provide the necessary Infrastructure to fully support encrypted transmissions.
- Third Parties – Third Parties who store or process Confidential or Restricted information must either meet the requirements of these standards or provide comparable controls validated by an IS assessment and accepted by the Business. (Such information must be encrypted in transit to and from the Third Party when sent electronically.)
- Voice and Fax – Confidential or Restricted information sent over Fax or discussed on voice calls (including Voice Over IP [VOIP]) may be sent unencrypted. Businesses should develop specific procedures and guidance to protect Confidential and Restricted information sent via these channels.

Appendix B: Schedule of Associated Documents:

- Citigroup 3rd Party Access Registry (C3PAR)
(<http://www.citigroup.net/informationsecurityservices/tpaswg/index.htm>)
- Citigroup Information Technology Management Policy (CITMP)
(http://www.citigroup.net/policydirectory/index_otp.htm)
- Citigroup Records Management Policy and Standards
(http://globalcompliance.nj.ssmb.com/data/compl/univ_record.htm)
- Common Risk Assessment Process
(<http://www.citigroup.net/informationsecurityservices/exco/index.htm#cra>)
- Database Security Guidelines
(http://www.citigroup.net/informationsecurityservices/doc/istg/Database_Security_Guidelines_V3-1.pdf)
- Electronic Communications Policy
(<http://www.citigroup.net/citigrouptoday/announcement/ann050407d.shtml>)
- Electronic Transportable Media (ETM) Standards
(http://www.citigroup.net/informationsecurityservices/data/exco/ETM_Standards_17-Jan-20061.doc)
- Global Security Policy (http://www.citigroup.net/csis/pdf/global_security_policy.pdf)
- Information Security Assessment Process for Mergers, Acquisitions, and Divestitures (MAD)
([Simulated Link](#))
- Information Security Risk Assessment (ISRA) Process
(<http://www.citigroup.net/informationsecurityservices/exco/index.htm#cra>)
- ISTG-Approved Citigroup Application Vulnerability Assessment Process ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Authentication ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Cryptography ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Developer Access to Controlled Information Systems
([Simulated Link](#))
- ISTG-Approved Technical Requirements for Functional IDs ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Inter-Corporation Network Connectivity ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Master IDs ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Network Security Domains ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Network Security Systems ([Simulated Link](#))
- ISTG-Approved Technical Requirements for Perimeters ([Simulated Link](#))

- ISTG-Approved Trusted Network Process ([Simulated Link](#))
- Risk Control Self Assessment (RCSA) Process
(http://www.citigroup.net/riskarchitecture/rcsa_orps.htm)
- Security Incident Response Team (SIRT) Process
(http://www.citigroup.net/informationsecurityservices/doc/citigroup_sirt_process.doc)
- Third Party Information Security Assessment (TPISA) Process
(<http://www.citigroup.net/informationsecurityservices/tpisa/index.htm>)
- Vendor Selection and Management Policy & Standards
(http://www.citigroup.net/policydirectory/pdf/operationsandtechnology/vendor_selection_and_management_policy.pdf)

Appendix C: Schedule of ISTG-Approved Technology:

ISTG-Approved Technologies can be found: <http://www.citigroup.net/informationsecurityservices/istg/index.htm>

- Anti virus products
- Anti spyware products
- Approved certificate authorities
- Authentication services
- Encryption algorithms
- Key management tools and techniques
- Remote access system
- Remote access portal
- Strong authentication
- Virtual Private Network (VPN)
- WLANs / wireless device solutions / instant messaging / peer to peer networks / internet collaborative tools

Appendix D: CISS Standard Statement to ISO17799 Control Statement Mapping

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
1.1	7.1.2	<u>Ownership of assets</u> All information and assets associated with information processing facilities should be owned by a designated part of the organization.
1.2	7.2.1	<u>Classification guidelines</u> Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
1.3	6.1.2	<u>Information security co-ordination</u> Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
1.4	6.1.1	<u>Management commitment to information security</u> Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
1.4	7.2.1	<u>Classification guidelines</u> Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
1.4	7.2.2	<u>Information labeling and handling</u> An appropriate set of procedures for information labeling and handling should be developed.
1.5	7.1.1	<u>Inventory of assets</u> All assets should be clearly identified and an inventory of all important assets drawn up and maintained.
1.6, 1.7, 1.8	11.4.5	<u>Segregation in networks</u> Groups of information services, users, and information systems should be segregated on networks.
1.9	9.1.1	<u>Physical security perimeter</u> Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.
2.1, 2.2	11.5.2	<u>User identification and authentication</u> All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
2.3	11.4.3	<u>Equipment identification in networks</u> Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
2.4	7.1.3	<u>Acceptable use of assets</u> Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.
2.5, 2.6	11.3.1	<u>Password use</u> Users should be required to follow good security practices in the selection and use of passwords.
2.5, 2.6	11.5.3	<u>Password management system</u>

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
		Systems for managing passwords should be interactive and should ensure quality passwords.
2.7	10.9.2	<u>On-Line Transactions</u> Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
2.7	11.4.2	<u>User authentication for external connections</u> Appropriate authentication methods should be used to control access by remote users.
2.8	11.5.1	<u>Secure log-on procedures</u> Access to operating systems should be controlled by a secure log-on procedure.
2.9	11.2.3	<u>User password management</u> The allocation of passwords should be controlled through a formal management process.
2.9	11.5.3	<u>Password management system</u> Systems for managing passwords should be interactive and should ensure quality passwords.
2.10	10.1.3	<u>Segregation of duties</u> Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
2.10	10.6.1	<u>Network controls</u> Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
2.10	10.10.1	<u>Audit logging</u> Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
2.10	11.4.2	<u>User authentication for external connections</u> Appropriate authentication methods should be used to control access by remote users.
2.10	11.4.5	<u>Segregation in networks</u> Groups of information services, users, and information systems should be segregated on networks.
2.11	10.9.2	<u>On-Line Transactions</u> Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
2.11	11.5.2	<u>User identification and authentication</u> All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
2.12	11.2.3	<u>User password management</u> The allocation of passwords should be controlled through a formal management process.

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
2.12	11.5.3	<u>Password management system</u> Systems for managing passwords should be interactive and should ensure quality passwords.
3.1	11.2.4	<u>Review of user access rights</u> Management should review users' access rights at regular intervals using a formal process.
3.1	11.1.1	<u>Access control policy</u> An access control policy should be established, documented, and reviewed based on business and security requirements for access.
3.1	11.2.2	<u>Privilege management</u> The allocation and use of privileges should be restricted and controlled.
3.2	10.6.1	<u>Network controls</u> Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
3.2	11.1.1	<u>Access control policy</u> An access control policy should be established, documented, and reviewed based on business and security requirements for access.
3.2	11.5.4	<u>Use of system utilities</u> The use of system utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.
3.2	11.6.1	<u>Information access restriction</u> Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.
3.3	11.2.4	<u>Review of user access rights</u> Management should review users' access rights at regular intervals using a formal process.
3.4	10.1.3	<u>Segregation of duties</u> Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
3.4	11.2.4	<u>Review of user access rights</u> Management should review users' access rights at regular intervals using a formal process.
3.5	8.3.1	<u>Termination responsibilities</u> Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.
3.5	8.3.3	<u>Removal of access rights</u> The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.
3.5	11.2.1	<u>User registration</u> There should be a formal user registration and de-registration procedure in place for granting and revoking access to all

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
		information systems and services.
3.5	11.2.2	<u>Privilege management</u> The allocation and use of privileges should be restricted and controlled.
3.5	11.2.4	<u>Review of user access rights</u> Management should review users' access rights at regular intervals using a formal process.
3.6	11.5.1	<u>Secure log-on procedures</u> Access to operating systems should be controlled by a secure log-on procedure.
3.6	15.1.5	<u>Prevention of misuse of information processing facilities</u> Users should be deterred from using information processing facilities for unauthorized purposes.
3.7	11.4.2	<u>User authentication for external connections</u> Appropriate authentication methods should be used to control access by remote users.
3.7	11.7.1	<u>Mobile computing and communications</u> A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
3.8	6.2	<u>External Parties</u> ...Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled... Controls should be agreed and defined in an agreement with the external party.
3.9	6.2.3	<u>Addressing security in third party agreements</u> Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.
3.9	7.2.2	<u>Information labeling and handling</u> An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.
3.9	8.1.3	<u>Terms and conditions of employment</u> As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.
3.10	11.4.2	<u>User authentication for external connections</u> Appropriate authentication methods should be used to control access by remote users.
3.10	11.7.2	<u>Teleworking</u> A policy, operational plans and procedures should be developed and implemented for teleworking activities.
3.11	7.1.3	<u>Acceptable use of assets</u> Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
3.11	7.2.2	<u>Information labeling and handling</u> An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.
3.11	8.2.2	<u>Information security awareness, education, and training</u> All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
3.11	10.8.4	<u>Electronic messaging</u> Information involved in electronic messaging should be appropriately protected.
3.11	11.4.1	<u>Policy on use of network services</u> Users should only be provided with access to the services that they have been specifically authorized to use.
3.11	11.7.1	<u>Mobile computing and communications</u> A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
3.12	11.4.3	<u>Equipment identification in networks</u> Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
4.1	7.1.3	<u>Acceptable use of assets</u> Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.
4.2, 4.3	10.7.3	<u>Information handling procedures</u> Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.
4.2, 4.3	10.7.1	<u>Management of removable media</u> There should be procedures in place for the management of removable media.
4.3	12.3.1	<u>Policy on the use of cryptographic controls</u> A policy on the use of cryptographic controls for protection of information should be developed and implemented.
4.4	7.2.2	<u>Information labeling and handling</u> An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.
4.4	11.3.3	<u>Clear desk and clear screen policy</u> A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.
4.5	10.7.2	<u>Disposal of media</u> Media should be disposed of securely and safely when no longer required, using formal procedures.
4.6	10.4.1	<u>Controls against malicious code</u> Detection, prevention, and recovery controls to protect against

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
		malicious code and appropriate user awareness procedures should be implemented.
4.7	10.4.2	<u>Controls against mobile code</u> Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.
4.8	6.2.3	<u>Addressing security in third party agreements</u> Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.
4.8	8.1.3	<u>Terms and conditions of employment</u> As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.
4.8	12.4.1	<u>Control of operational software</u> There should be procedures in place to control the installation of software on operational systems.
4.9	6.2.1	<u>Identification of risks related to external parties</u> The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.
4.9	6.2.2	<u>Addressing security when dealing with customers</u> All identified security requirements should be addressed before giving customers access to the organization's information or assets.
4.9	10.2.2	<u>Monitoring and review of third party services</u> The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.
5.1	13.1.1	<u>Reporting information security events</u> Information security events should be reported through appropriate management channels as quickly as possible.
5.1	13.1.2	<u>Reporting security weaknesses</u> All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.
5.2, 5.3	13.1.1	<u>Reporting information security events</u> Information security events should be reported through appropriate management channels as quickly as possible.
5.3	8.2.2	<u>Information security awareness, education, and training</u> All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
5.3	13.1.2	<u>Reporting security weaknesses</u> All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.
5.3	13.2.1	<u>Responsibilities and procedures</u> Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.
6.1	8.1.2	<u>Screening</u> Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
6.2	12.1.1	<u>Security requirements analysis and specification</u> Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.
6.3, 6.4	10.1.3	<u>Segregation of duties</u> Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
6.5	6.2.3	<u>Addressing security in third party agreements</u> Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.
6.5	10.2.1	<u>Service delivery</u> It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
6.6	15.2.2	<u>Technical compliance checking</u> Information systems should be regularly checked for compliance with security implementation standards.
6.7	6.2.3	<u>Addressing security in third party agreements</u> Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.
6.8	15.2.1	<u>Compliance with security policies and standards</u> Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
7.1, 7.2, 7.3	8.2.2	<u>Information security awareness, education, and training</u> All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
		policies and procedures, as relevant for their job function.
8.1, 8.2, 8.3	12.6.1	<u>Control of technical vulnerabilities</u> Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
9.1	12.3.2	<u>Key management</u> Key management should be in place to support the organization's use of cryptographic techniques.
9.2	12.3.1	<u>Policy on the use of cryptographic controls</u> A policy on the use of cryptographic controls for protection of information should be developed and implemented.
10.1, 10.2	11.4.6	<u>Network connection control</u> For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.
10.1	10.6.1	<u>Network controls</u> Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
10.1	10.8.5	<u>Business information systems</u> Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.
10.2	10.6.1	<u>Network controls</u> Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
10.3	12.5.1	<u>Change control procedures</u> The implementation of changes should be controlled by the use of formal change control procedures.
10.4	13.2.1	<u>Responsibilities and procedures</u> Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.
10.5	10.8.5	<u>Business information systems</u> Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.
10.6	10.10.1	<u>Audit logging</u> Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
10.6	10.10.2	<u>Monitoring system use</u> Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.
10.7	13.2.1	<u>Responsibilities and procedures</u>

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
		Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.
10.8	10.6.1	<u>Network controls</u> Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
10.8	10.8.5	<u>Business information systems</u> Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.
11.1	10.10.1	<u>Audit logging</u> Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
11.1	10.10.4	<u>Administrator and operator logs</u> System administrator and system operator activities should be logged.
11.1	10.10.6	<u>Clock synchronization</u> The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.
11.2	10.1.3	<u>Segregation of duties</u> Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
11.2	10.10.1	<u>Audit logging</u> Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
11.2	13.1.1	<u>Reporting information security events</u> Information security events should be reported through appropriate management channels as quickly as possible.
12.1	10.1.4	<u>Separation of development, test, and operational facilities</u> Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.
12.1, 12.2	11.1.1	<u>Access control policy</u> An access control policy should be established, documented, and reviewed based on business and security requirements for access.
12.3	12.4.2	<u>Protection of system test data</u> Test data should be selected carefully, and protected and controlled.
12.4	10.1.4	<u>Separation of development, test, and operational facilities</u> Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.
13.1	7.1.1	<u>Inventory of assets</u>

CISS Standard Number	ISO17799 Reference Number	ISO17799 Control Statement
		All assets should be clearly identified and an inventory of all important assets drawn up and maintained.
13.1	15.2.2	<u>Technical compliance checking</u> Information systems should be regularly checked for compliance with security implementation standards.