Statement of Applicability

Current as of:
October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
5. Security Policy	5.1	Information Security Policy							
	5.1.1	Information Security Policy Document	■	Existing controls			■	■	highlight the importance of having secured communications while doing business online
	5.1.2	Review of Information Security Policy	■	SOC			■		1. Internal review by IT Security Office and CIO. 2. Reviews by bank committees, peer groups
6. Organization of Information security	6.1	Internal Organization							
	6.1.1	Management Commitment to information security							
	6.1.2	Information security Co-ordination							
	6.1.3	Allocation of information security Responsibilities							
	6.1.4	Authorization process for Information Processing facilities	■	Existing controls			■		'1. Criteria must be established by the Data Owner for account eligibility, creation,maintenance, and expiration. 2. Physical access should be monitored, and access records maintained.
	6.1.5	Confidentiality agreements							
	6.1.6	Contact with authorities							
	6.1.7	Contact with special interest groups	■	Existing controls		■	■	■	Creating a support network of other security specialists.
	6.1.8	Independent review of information security							
	6.2	External Parties							
	6.2.1	Identification of risk related to external parties							
	6.2.2	Addressing security when dealing with customers							

Statement of Applicability

Current as of:
October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
	6.2.3	Addressing security in third party agreements	■			■	■	■	Agreements with third parties involving accessing, processing, communicating or managing the bank's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements
7. Asset Management	7.1	Responsibility for Assets							
	7.1.1	Inventory of assets							
	7.1.2	Ownership of Assets	■	Existing controls			■		Asset Register - Designating Information Custodians and ensuring that they have the correct tools for protecting designated assets
	7.1.3	Acceptable use of assets							
	7.2	Information classification							
	7.2.1	Classification Guidelines							
	7.2.2	Information Labeling and Handling							
8. Human Resource Security	8.1	Prior to Employment							
	8.1.1	Roles and Responsibilities	■	Existing controls			■		Information Owners and Information Custodians must: □ Document information security roles and responsibilities for personnel in job descriptions, standing offers, contracts, and information use agreements; and, □ Review and update information security roles and responsibilities when conducting staffing or contracting activities
	8.1.2	Screening							
	8.1.3	Terms and conditions of employment							
	8.2	During Employment							
	8.2.1	Management Responsibility							
	8.2.2	Information security awareness, education and training							
	8.2.3	Disciplinary process							
	8.3	Termination or change of employment							
	8.3.1	Termination responsibility							
	8.3.2	Return of assets							

Statement of Applicability

Current as of: October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
	8.3.3	Removal of access rights	■	Existing controls			■	■	Managers must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment by: □ Removing or modifying physical and logical access; □ Recovering or revoking access devices, cards and keys; and, □ Updating directories, documentation and systems.
9. Physical and Environmental Security	9.1	Secure Areas							
	9.1.1	Physical security Perimeter	■	Existing controls		■			
	9.1.2	Physical entry controls	■	Existing controls		■		■	Implement swipe card on all data centers and established visitor control logs
	9.1.3	Securing offices, rooms and facilities	■	Existing controls				■	
	9.1.4	Protecting against external and environmental threats	■	Existing controls					
	9.1.5	Working in secure areas	■	Existing controls					Policy created
	9.1.6	Public access, delivery and loading areas	■	Existing controls					
	9.2	Equipment security							
	9.2.1	Equipment sitting and protection	■	Existing controls		■		■	
	9.2.2	Support utilities	■	Existing controls				■	
	9.2.3	Cabling security	■	Existing controls		■			
	9.2.4	Equipment Maintenance	■	Existing controls		■		■	Formalized PM mechanism
	9.2.5	Security of equipment off-premises	■	Existing controls					
	9.2.6	Secure disposal or reuse of equipment							Implemented procedure
	9.2.7	Removal of Property	■	Existing controls. Use of gate pass.					
	10.1	Operational Procedures and responsibilities							
	10.1.1	Documented operating Procedures							

Statement of Applicability

Current as of:
October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
	10.1.2	Change Management	■	Existing controls		■	■		Information Owners and Information Custodians must implement changes by: □ Notifying affected parties, including business partners and third parties; □ Completing re-certification and re-accreditation as required prior to implementation; □ Training users if required; □ Documenting and reviewing the documentation throughout the testing and implementation phases; □ Recording all pertinent details regarding the changes;
	10.1.3	Segregation of Duties							
	10.1.4	Separation of development and Operations facilities							
	10.2	Third Party Service Delivery Management							
	10.2.1	Service Delivery							
	10.2.2	Monitoring and review of third party services							
	10.2.3	Manage changes to the third party services							
	10.3	System Planning and Acceptance							
	10.3.1	Capacity management							
	10.3.2	System acceptance	■	Existing controls		■		■	Prior to implementing new or upgraded information systems, bord of directors must ensure: □ Acceptance criteria are identified including privacy, security, systems development and user acceptance testing; □ Security certification is attained, indicating the system meets minimum acceptance criteria;
	10.4	Protection against Malicious and Mobile Code							
	10.4.1	Controls against malicious code							
	10.4.2	Controls against Mobile code		unattended and no previous attacks on this					
	10.5	Back-Up							
	10.5.1	Information Backup							
	10.6	Network Security Management							
	10.6.1	Network controls							
	10.6.2	Security of Network services	■	Existing controls	■			■	Implement Network service agreement
	10.7	Media Handling							

Statement of Applicability

Current as of:
October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
10. Communications and Operations Management	10.7.1	Management of removable media							
	10.7.2	Disposal of Media							
	10.7.3	Information handling procedures	■	Existing controls			■	■	□ Marking of media to its maximum information classification level label, in order to indicate the sensitivity of information contained on the media; □ Access control restrictions and authorization; □ Correct use of technology (e.g., encryption) to enforce access control; □ Copying and distribution of media, including minimization of multiple copies, marking of originals and distribution of copies;
	10.7.4	Security of system documentation							
	10.8	Exchange of Information							
	10.8.1	Information exchange policies and procedures							
	10.8.2	Exchange agreements							
	10.8.3	Physical media in transit							
	10.8.4	Electronic Messaging	■	Existing controls			■	■	Personnel must support the responsible use of electronic messaging services by: □ Using only government electronic messaging systems, including systems for remote access to government messaging systems from publicly available networks; □ Using only authorized encryption for e-mail or attachments; and □ Not automatically forwarding government e-mail to external e-mail addresses;
	10.8.5	Business Information systems							
	10.9	Electronic Commerce Services							
	10.9.1	Electronic Commerce							
	10.9.2	On-Line transactions							

Statement of Applicability

Current as of: October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
	10.9.3	Publicly available information	■	Existing controls			■	■	Information Owners must approve the publication, modification or removal of information on publicly available information systems. Information Custodians are responsible for maintaining the accuracy and integrity of the published information Maintain a record of changes to published information; Maintain the integrity of published information; Prevent the inappropriate release of sensitive or personal information; Monitor for unauthorized changes; and, Prevent unauthorized access to networks and information systems
	10.10	Monitoring							
	10.10.1	Audit logging							
	10.10.2	Monitoring system use	■	Existing controls		■		■	Process management ensure that the use of information systems can be monitored to detect activities including: authorized and unauthorized accesses, system alerts and failures System Admin must implement, manage and monitor logging systems for: Authorized access, Privileged operations, Unauthorized access attempts, System alerts or failures
	10.10.3	Protection of log information							
	10.10.4	Administrator and operator logs							
	10.10.5	Fault logging							
	10.10.6	Clock synchronization	■	Existing controls			■		System administrators must synchronize information system clocks to: the local router gateway; or, government approved clock host
	11.1	Business Requirement for Access Control							
	11.1.1	Access control Policy							
	11.2	User Access Management							
	11.2.1	User Registration							
	11.2.2	Privilege Measurement							
	11.2.3	User password management							
	11.2.4	Review of user access rights							
	11.3	User Responsibilities							
	11.3.1	Password Use							
	11.3.2	Unattended user equipment							

Statement of Applicability

Current as of: October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
11. Access control	11.3.3	Clear Desk and Clear Screen Policy							
	11.4	Network Access control							
	11.4.1	Policy on use of network services							
	11.4.2	User authentication for external connections							
	11.4.3	Equipment identification in networks							
	11.4.4	Remote diagnostic and configuration port protection							
	11.4.5	Segregation in networks							
	11.4.6	Network connection control							
	11.4.7	Network Routing control							
	11.5	Operating System Access Control							
	11.5.1	Secure Log-on procedures							
	11.5.2	User identification and authentication							
	11.5.3	Password Management system							
	11.5.4	Use of system utilities							
	11.5.5	Session Time-out							
	11.5.6	Limitation of connection time							
	11.6	Application access control							
	11.6.1	Information access restriction							
	11.6.2	Sensitive system isolation							
	11.7	Mobile Computing and Teleworking							
	11.7.1	Mobile computing and communication							
	11.7.2	Teleworking							
12. Information Systems Acquisition Development and Maintenance	12.1	Security Requirements of Information Systems							
	12.1.1	Security requirement analysis and specifications							
	12.2	Correct Processing in Applications							
	12.2.1	Input data validation							
	12.2.2	Control of internal processing							
	12.2.3	Message integrity							
	12.2.4	Output data validation							
	12.3	Cryptographic controls							
	12.3.1	Policy on the use of cryptographic controls							
	12.3.2	Key Management							
	12.4	Security of System Files							
	12.4.1	Control of Operational software							
	12.4.2	Protection of system test data							
	12.4.3	Access control to program source library							
	12.5	Security in Development & Support Processes							
	12.5.1	Change Control Procedures							
	12.5.2	Technical review of applications after Operating system changes							
	12.5.3	Restrictions on changes to software packages							

Statement of Applicability

Current as of:
October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
	12.5.4	Information Leakage							
	12.5.5	Outsourced Software Development							
	12.6	Technical Vulnerability Management							
	12.6.1	Control of technical vulnerabilities							
13. Information Security Incident Management	13.1	Reporting Information Security Events and Weaknesses							
	13.1.1	Reporting Information security events							
	13.1.2	Reporting security weaknesses							
	13.2	Management of Information Security Incidents and Improvements							
	13.2.1	Responsibilities and Procedures							
	13.2.2	Learning for Information security incidents							
	13.2.3	Collection of evidence							
14. Business Continuity Management	14.1	Information Security Aspects of Business Continuity Management							
	14.1.1	Including Information Security in Business continuity management process							
	14.1.2	Business continuity and Risk Assessment							
	14.1.3	developing and implementing continuity plans including information security							
	14.1.4	Business continuity planning framework							
	14.1.5	Testing, maintaining and re-assessing business continuity plans							
15. Compliance	15.1	Compliance with Legal Requirements							
	15.1.1	Identification of applicable legislations							
	15.1.2	Intellectual Property Rights (IPR)							
	15.1.3	Protection of organizational records							
	15.1.4	Data Protection and privacy of personal information							
	15.1.5	Prevention of misuse of information processing facilities							
	15.1.6	Regulation of cryptographic controls							
	15.2	Compliance with Security Policies and Standards and Technical compliance							
	15.2.1	Compliance with security policy							
	15.2.2	Technical compliance checking							
	15.3	Information System Audit Considerations							
	15.3.1	Information System Audit controls							
	15.3.2	Protection of information system audit tools							

Statement of Applicability

Current as of:
October 2012

Legend (for Selected Controls and Reasons for controls selection)
LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							