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							
	5.1	Information Security Policy							
5. Security Policy	5.1.1	Information Security Policy Document	▪	Existing controls			▪	▪	Access level is implemented and the creation of a security policy is to set a company's information security foundations, to explain to staff how they are responsible for the protection of the information resources, and 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 campus committees, peer groups and University Senate.
	6.1	Internal Organization							
6. Organization of Information security	6.1.1	Management Commitment to information security	▪	Existing controls			▪		Management should approve the information security policy, assign security roles and co-ordinate and review the implementation of security across the organization.
	6.1.2	Information security Co-ordination							
	6.1.3	Allocation of information security Responsibilities	▪	Existing controls		▪	▪	▪	heads of department are responsible for information security within their departments
	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	▪	Existing controls	▪				The Recipient agrees not to disclose the confidential information obtained from the discloser to anyone unless required to do so by law.
	6.1.6	Contact with authorities	▪	Existing controls	▪				Appropriate contacts shall be maintained with local law enforcement authorities, emergency support staff and service providers.
	6.1.7	Contact with special interest groups	▪	Existing controls		▪	▪	▪	1. Participating in information exchange forums regarding best practices, industry standards development, new technologies, threats, vulnerabilities, early notice of potential attacks, and advisories; 2. Creating a support network of other security specialists.
	6.1.8	Independent review of information security	▪	Existing controls			▪		The Chief Information Security Officer must initiate an independent review of the Information Security Program every two years including: ▪ Assessing the operational effectiveness of the Information Security Program; ▪ Documenting the results; and, ▪ Reporting the results of the review to senior management.
	6.2	External Parties							
	6.2.1	Identification of risk related to external parties	▪	Existing controls		▪	▪	▪	
	6.2.2	Addressing security when dealing with customers							
	6.2.3	Addressing security in third party agreements	▪	Existing controls		▪	▪	▪	Agreements with third parties involving accessing, processing, communicating or managing the University's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements
	7.1	Responsibility for Assets							
7. Asset Management	7.1.1	Inventory of assets	▪	Existing controls	▪		▪		Risk Assessment Report And Asset Register
	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	▪	Existing controls			▪		
	7.2	Information classification							
	7.2.1	Classification Guidelines	▪	Existing controls			▪		1.Information and information system security classification 2. Mandatory features of information
	7.2.2	Information Labeling and Handling		Unnecessary Process					
	8.1	Prior to Employment							

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. Human Resource Security	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	▪	Existing controls		▪	▪		have formal interviews
	8.1.3	Terms and conditions of employment	▪	Existing controls		▪	▪		have formal interviews
	8.2	During Employment							
	8.2.1	Management Responsibility	▪	Existing controls	▪		▪		1. development of policies is the responsibility of the Chief Information Security Officer. University senior management and executive Director of risk management and safty service provide advice for new security issues. 2. Review of security roles and responsibilities
	8.2.2	Information security awareness, education and training	▪	Existing controls	▪	▪	▪		Managers must provide ongoing information security awareness, education and training, addressing topics including: Protection of information; Known information security threats; Legal responsibilities; Information security policies and directives
	8.2.3	Disciplinary process	▪	Existing controls	▪		▪	▪	
	8.3	Termination or change of employment							
	8.3.1	Termination responsibility							
	8.3.2	Return of assets	▪	Existing controls	▪		▪		according to he document of return on Assets and procedure
	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	▪	Existing controls			▪		Information Custodians must ensure that approved operating procedures and standards are: Documented; Consistent with government policies; Reviewed and updated annually;

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	▪	Existing controls			▪	▪	Requiring that no single individual has access to all operational functions of an information system (e.g., operating system administrators must not also have application administrator privileges);
	10.1.4	Separation of development and Operations facilities	▪	Existing controls			▪	▪	Information Custodians must protect operational information systems by: □ Separating operational environments from test and development environments using different computer rooms, servers, domains and partitions;
	10.2	Third Party Service Delivery Management							
	10.2.1	Service Delivery	▪	Existing controls	▪			▪	senior management must ensure service agreements with external parties document service level continuity requirements and include processes for: □ Ongoing review of service level needs with business process owners; □ Audit and compliance monitoring rights and responsibilities; □ Communicating requirements to service providers;
	10.2.2	Monitoring and review of third party services	▪	Existing controls				▪	based on Service Delivery Agreements
	10.2.3	Manage changes to the third party services	▪	Existing controls	▪			▪	based on Service Delivery Agreements (must ensure agreements with external party service providers include provisions for: □ Amending agreements when required by changes to legislation, regulation, business requirements, policy or service delivery; and, □ Requiring the service provider to obtain pre-approval for significant changes involving: o Network services, o New technologies)
	10.3	System Planning and Acceptance							
	10.3.1	Capacity management	yes				▪	▪	Resource capacity management - for implementing capacity management processes by: □ Documenting capacity requirements and capacity planning processes, □ Including capacity requirements in service agreements; □ Monitoring and optimizing information systems to detect impending capacity limits;
	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							

Statement of Applicability

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

Current as of:
October 2012

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	10.4.1	Controls against malicious code	▪	Existing controls				▪	The Chief Information Security Officer must ensure processes are implemented to: □ Maintain a critical incident management plan to identify and respond to malicious code incidents; and, □ Maintain a register of specific malicious code countermeasures (e.g., blocked websites, blocked electronic mail attachment file types and blocked network ports) □ Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from 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	▪	Existing controls			▪	▪	Safeguarding backup facilities and media -□ Using encryption to protect the backed up information; □ Using digital signatures to protect the integrity of the information; □ Physical and environmental security; □ Access controls; □Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.
	10.6	Network Security Management							
	10.6.1	Network controls	▪	Existing controls	▪		▪	▪	Wireless Local Area Networking -- Wireless Local Area Networks must utilize the controls specified by the Chief Information Security Officer and must include: □ Strong link layer encryption, such as Wi-Fi Protected Access; □ User and device network access controlled by government authentication services; □ The use of strong, frequently changed, automatically expiring encryption keys and passwords; □ Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies;
	10.6.2	Security of Network services	▪	Existing controls	▪			▪	Implement Network service agreement
	10.7	Media Handling							
	10.7.1	Management of removable media	▪					▪	Information Owners, Information Custodians and Managers must: □ Ensure that use of portable storage devices is managed and controlled to mitigate risks; □ Document processes for authorizing use of portable storage devices; and, □ Ensure personnel using portable storage devices protect information and information technology assets in their custody or control.
	10.7.2	Disposal of Media		not existing					
	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	▪	Existing controls	▪		▪	▪	□ Establish lists of users authorized to access system documentation and Require use of access controls, passwords, encryption or digital signatures as appropriate to the information classification;
	10.8	Exchange of Information							

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**							
	10.8.1	Information exchange policies and procedures	▪	Existing controls				▪	The Chief Information Security Officer must document and implement procedures to protect information from interception, copying, misrouting and destruction when being transmitted electronically or verbally.
	10.8.2	Exchange agreements			▪			▪	Information Owners and Information Custodians must ensure the following are completed for the information or software covered by the exchange agreement: □ An approved Privacy Impact Assessment; and, □ A Security Threat and Risk Assessment.
	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	▪	Existing controls			▪	▪	Implement procedures to restrict access to information in interconnected internal administrative and productivity information systems that support government such as e-mail, calendars and financial systems.
	10.9	Electronic Commerce Services							
	10.9.1	Electronic Commerce		not defined					
	10.9.2	On-Line transactions	▪	Existing controls	▪		▪	▪	transaction management are responsible for ensuring that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry Data Security Standard.
	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	▪	Existing controls	▪		▪	▪	Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs Audit logs must be: □ Retained according to the approved records retention schedule for the system or information asset; and, □ Retained indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

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**							
	10.10.2	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	▪	Existing controls			▪	▪	System Admin must implement controls to protect logging facilities and log files from unauthorized modification, access or destruction. Controls must include: □ Physical security safeguards such as situating logging facilities within a secure zone with restricted access; □ Administrators and operators must not have permission to erase or de-activate logs of their own activities; □ Consideration of multi-factor authentication for access to sensitive records; □ Back-up of audit logs to off-site facilities; □ Automatic archiving of audit logs to remain within storage capacity;
	10.10.4	Administrator and operator logs	▪	Existing controls			▪	▪	System Operation manager must ensure that the activities of privileged users are regularly reviewed including logging: □ Event occurrence times; □ Event details, such as files accessed, modified or deleted, errors and corrective action. □ Independent review.
	10.10.5	Fault logging	▪				▪		Authentication administrator must Reporting and logging faults and Analysis, resolution and corrective action.
	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	▪	Existing controls			▪	▪	Access control policies must additionally: □ Consider both physical and logical access to assets; □ Apply the “need to know” and “least privilege” principles; □ Set default access privileges to “deny-all” prior to granting access; □ Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable System administrator must conduct periodic reviews of the access control policy as part of an ongoing process for risk management, security, and privacy.
	11.2	User Access Management							
	11.2.1	User Registration	▪	Existing controls	▪		▪	▪	Access control management are responsible for managing access to the assets under their control and must implement registration processes which: □ Requires custodians to approve all access rights. □ Maintain records of access right approvals; □ Ensures personnel understand the conditions of access and, when appropriate, have signed confidentiality agreements; Promptly review access rights whenever a user changes duties and responsibilities;

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**							
	11.2.2	Privilege Measurement	▪	Existing controls			▪	▪	Access control management are responsible for authorizing system privileges and must: □ Identify and document the system privileges associated with each information system or service; □ Ensure the process for requesting and approving access to system privileges includes management approval(s) prior to granting of system privileges; □ Ensure processes are implemented to remove system privileges from users concurrent with changes in job status
	11.2.3	User password management	▪	Existing controls			▪	▪	Management must formally designate individuals who have the authority to issue and reset passwords. The following applies: □ Passwords shall only be issued to users whose identity is confirmed prior to issuance; □ Individuals with the authority to reset passwords must transmit new or reset passwords to the user in a secure manner (e.g., using encryption) □ Whenever technically possible temporary passwords must be unique to each individual and must not be easily guessable.
	11.2.4	Review of user access rights	▪	Existing controls			▪	▪	Circumstances and criteria for formal access right review - Authentication Administrator must implement formal processes for the regular review of access rights. Access rights must be reviewed: □ Annually; □ More frequently for high value information assets and privileged users; □ When a user's status changes as the result of a promotion, demotion, removal from a user group,
	11.3	User Responsibilities							
	11.3.1	Password Use	▪	Existing controls			▪	▪	Authentication administrator's responsibility --**When selecting passwords users must:** □ Select complex passwords, i.e., a mixture of characters as specified in the Standard; and, □ Avoid using the same password for multiple accounts. **Passwords must be changed**: □ During installation of computer hardware and or software which is delivered with a default password; **Privileged accounts:** □ Use passwords which are at least 15 characters where technically feasible; and, □ Change passwords more frequently than a password for normal account.
	11.3.2	Unattended user equipment	▪	Existing controls			▪	▪	every valuble person must ensure that users prevent unauthorized access to information systems by securing unattended equipment, by: □ Locking or terminating information system sessions before leaving the equipment unattended; □ Enabling a password protection features on the equipment (e.g., screen savers on workstations); □ Shutting down and restarting unattended workstations at the end of each workday; □ Enabling password protection on mobile devices including portable storage devices;
	11.3.3	Clear Desk and Clear Screen Policy	yes	not a defined control			▪	▪	Securing the work space includes: □ Clearing desk tops and work areas; □ Securing documents and portable storage devices in a locked desk or file cabinet; □ Ensure outgoing and incoming mail is appropriately secured; □ Enabling a password protected screen saver;
	11.4	Network Access control							

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	11.4.1	Policy on use of network services	▪		▪		▪	▪	Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers. Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system. Information Custodians must define and implement: Permitted network access methods for each network zone (e.g., direct connection, Virtual Private Network, dial-up); and, Minimum security controls required for connection to networks (e.g., patch levels, anti-virus software, firewalls, user and system authentication requirements).
	11.4.2	User authentication for external connections	▪	Existing controls			▪	▪	Require remote users to connect through government designated remote access services or security gateways (e.g., Virtual Private Network, Desktop Terminal Services (DTS), Outlook Web Access); and, Require user identification and authorization prior to permitting each remote network connection
	11.4.3	Equipment identification in networks		not defined					
	11.4.4	Remote diagnostic and configuration port protection	▪	Existing controls			▪	▪	implemented access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities. Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.
	11.4.5	Segregation in networks	▪	Existing controls			▪	▪	network Administrator must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.
	11.4.6	Network connection control	▪	Existing controls			▪	▪	* Logical and physical network connection control - database server hardware should be placed in a network security zone to segregate it from direct network connections by user workstations * lnetwork Administrator must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a Security Threat and Risk Assessment
	11.4.7	Network Routing control	▪	Existing controls	▪		▪	▪	network administrator must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).
	11.5	Operating System Access Control							
	11.5.1	Secure Log-on procedures	▪	Existing controls			▪	▪	Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance; Record unsuccessful logon attempts; Allow a limited number of unsuccessful logon attempts;
	11.5.2	User identification and authentication	▪	Existing controls			▪	▪	User identifiers authenticated by means other than a password must use a mechanism approved by the Chief Information Officer. The documented and approved process for allocating and managing unique identifiers must include:

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							
	11.5.3	Password Management system	▪	Existing controls			▪	▪	**Enforcing quality password rules:** □ Enforce the use of individual user identifiers and passwords; □ Support user selection and change of passwords using the Complex Password Standard □ Prevent re-use of passwords for a specified number of times; □ Prevent passwords from being viewed on-screen; □ Store password files separately from application system data;
	11.5.4	Use of system utilities	▪	Existing controls			▪	▪	System Administrator must limit use of system utility programs by: □ Defining and documenting authorization levels; □ Restricting the number of users with access to system utility programs; □ Annually reviewing the status of users with permissions to use system utility programs;
	11.5.5	Session Time-out	▪	Existing controls			▪	▪	Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity commensurate with the: □ Risks related to the security zone; □ Classification of the information being handled; and, □ Risks related to the use of the equipment by multiple users.
	11.5.6	Limitation of connection time	▪	Existing controls			▪	▪	Information Security Administrator must limit the duration of connection times for high value applications. Restricting connection duration includes: □ Limiting session length; and, □ Requiring re-authentication of the user when a session has been inactive for a pre-defined period of time.
	11.6	Application access control							
	11.6.1	Information access restriction	▪	Existing controls			▪	▪	The access control policy must identify the information and system functions accessible by various classes of users. Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.
	11.6.2	Sensitive system isolation	▪	Existing controls			▪		**Segregation of sensitive information systems:** The information system classification level determines which network security zone the information system must reside.
	11.7	Mobile Computing and Teleworking							
	11.7.1	Mobile computing and communication	▪	Existing controls			▪	▪	□ Encryption of stored data to prevent information loss resulting from the theft of the mobile or remote device; □ Encryption of data transmitted via public network; □ Access control permissions on a portable storage device must be applied to prevent unauthorised access to information by system users, particularly for multi-user mobile systems; □ Regularly maintained data backups of information stored on portable storage devices using government backup facilities to protect against information loss;
	11.7.2	Teleworking		not defined					
	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							

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. Information Systems Acquisition Development and Maintenance	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							
	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							