Compliance Checklist

Reference		Compliance Assessment Area		Results	
Checklist	Standard	Section	Initial Assessment Points	Findings	Status
	A.5	Information Security Policies			
	A.5.1	Management direction for information security			
	A.5.1.1	Policies for information security	1. Do Security policies exist? 2. Are all policies approved by management? 3. Are policies properly communicated to employees?		0%
	A.5.1.2	Review of the policies for information security	1. Are security policies subject to review? 2. Are the reviews conducted at regular intervals? 3. Are reviews conducted when circumstances change?		0%
	A.6	Organisation of information security			
	A.6.1	Internal Organisation			
	A.6.1.1	Information security roles and responsibilities	Are responsibilities for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated to the relevant parties?		0%
	A.6.1.2	Segregation of duties	Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services?		0%
	A.6.1.3	Contact with authorities	1. Is there a procedure documenting when, and by whom, contact with relevant authorities (law enforcement etc.) will be made? 2. Is there a process which details how and when contact is required? 3. Is there a process for routine contact and intelligence sharing?		0%
	A.6.1.4	Contact with special interest groups	Do relevant individuals within the organisation maintain active membership in relevant special interest groups?		0%
	A.6.1.5	Information security in project management	Do all projects go through some form of information security assessment?		0%
	A.6.2	Mobile devices and teleworking			
	A.6.2.1	Mobile device policy	1. Does a mobile device policy exist? 2. Does the policy have management approval? 3. Does the policy document and address additional risks from using mobile devices (e.g. Theft of asset, use of open wireless hotspots etc.)		0%
	A.6.2.2	Teleworking	1. Is there a policy for teleworking? 2. Does this have management approval? 3. Is there a set process for remote workers to get access? 4. Are teleworkers given the advice and equipment to protect their assets?		0%
	A.7	Human resources security			
	A.7.1	Prior to employment			

	A.7.1.1	Screening	1. Are background verification checks carried out on all new candidates for employment? 2. Are these checks approved by appropriate management authority? 3. Are the checks compliant with relevant laws, regulations and ethics? 4. Are the level of checks required supported by business risk assessments?		0%
	A.7.1.2	Terms and conditions of employment	1. Are all employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? 2. Do employment / service contracts specifically cover the need to protect business information?		0%
	A.7.2	**During employment**			
	A.7.2.1	Management responsibilities	1. Are managers (of all levels) engaged in driving security within the business? 2. Does management behaviour and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures?		0%
	A.7.2.2	Information security awareness, education and training	Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the organisation?		0%
	A.7.2.3	Disciplinary process	1. Is there a formal disciplinary process which allows the organisation to take action against employees who have committed an information security breach? 2. Is this communicated to all employees?		0%
	A.7.3	**Termination and change of employment**			
	A.7.3.1	Termination or change of employment responsibilities	1. Is there a documented process for terminating or changing employment duties? 2. Are any information security duties which survive employment communicated to the employee or contractor? 3. Is the organisation able to enforce compliance with any duties that survive employment?		0%
	A.8	**Asset management**			
	A.8.1	**Responsibility for assets**			
	A.8.1.1	Inventory of assets	1. Is there an inventory of all assets associated with information and information processing facilities? 2. Is the inventory accurate and kept up to date?		0%
	A.8.1.2	Ownership of assets	All information assets must have a clearly defined owner who is aware of their responsibilities.		0%
	A.8.1.3	Acceptable use of assets	1. Is there an acceptable use policy for each class / type of information asset? 2. Are users made aware of this policy prior to use?		0%

	A.8.1.4	Return of assets	Is there a process in place to ensure all employees and external users return the organisation's assets on termination of their employment, contract or agreement?		0%
	A.8.2	**Information classification**			
	A.8.2.1	Classification of information	1. Is there a policy governing information classification? 2. Is there a process by which all information can be appropriately classified?		0%
	A.8.2.2	Labelling of information	Is there a process or procedure for ensuring information classification is appropriately marked on each asset?		0%
	A.8.2.3	Handling of assets	1. Is there a procedure for handling each information classification? 2. Are users of information assets made aware of this procedure?		0%
	A.8.3	**Media handling**			
	A.8.3.1	Management of removable media	1. Is there a policy governing removable media? 2. Is there a process covering how removable media is managed? 3. Are the policy and process(es) communicated to all employees using removable media?		0%
	A.8.3.2	Disposal of media	Is there a formal procedure governing how removable media is disposed?		0%
	A.8.3.3	Physical media transfer	1. Is there a documented policy and process detailing how physical media should be transported? 2. Is media in transport protected against unauthorised access, misuse or corruption?		0%
	A.9	**Access control**			
	A.9.1	**Business requirements for access control**			
	A.9.1.1	Access control policy	1. Is there a documented access control policy? 2. Is the policy based on business requirements? 3. Is the policy communicated appropriately?		0%
	A.9.1.2	Access to networks and network services	Are controls in place to ensure users only have access to the network resources they have been specially authorised to use and are required for their duties?		0%
	A.9.2	**User access management**			
	A.9.2.1	User registration and de-registration	Is there a formal user access registration process in place?		0%
	A.9.2.2	User access provisioning	Is there a formal user access provisioning process in place to assign access rights for all user types and services?		0%
	A.9.2.3	Management of privileged access rights	Are privileged access accounts separately managed and controlled?		0%
	A.9.2.4	Management of secret authentication information of users	Is there a formal management process in place to control allocation of secret authentication information?		0%

	A.9.2.5	Review of user access rights	1. Is there a process for asset owners to review access rights to their assets on a regular basis? 2. Is this review process verified?		0%
	A.9.2.6	Removal or adjustment of access rights	Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role?		0%
	A.9.3	**User responsibilities**			
	A.9.3.1	Use of secret authentication information	1. Is there a policy document covering the organisations practices in how secret authentication information must be handled? 2. Is this communicated to all users?		0%
	A.9.4	**System and application access control**			
	A.9.4.1	Information access restriction	Is access to information and application system functions restricted in line with the access control policy?		0%
	A.9.4.2	Secure log-on procedures	Where the access control policy requires it, is access controlled by a secure log-on procedure?		0%
	A.9.4.3	Password management system	1. Are password systems interactive? 2. Are complex passwords required?		0%
	A.9.4.4	Use of privileged utility programs	Are privilege utility programs restricted and monitored?		0%
	A.9.4.5	Access control to program source code	Is access to the source code of the Access Control System protected?		0%
	A.10	**Cryptography**			
	A.10.1	**Cryptographic controls**			
	A.10.1.1	Policy on the use of cryptographic controls	Is there a policy on the use of cryptographic controls?		0%
	A.10.1.2	Key management	Is there a policy governing the whole lifecycle of cryptographic keys?		0%

	A.11	**Physical and environmental security**			
	A.11.1	**Secure areas**			
	A.11.1.1	Physical security perimeter	1. Is there a designated security perimeter? 2. Are sensitive or critical information areas segregated and appropriately controlled?		0%
	A.11.1.2	Physical entry controls	Do secure areas have suitable entry control systems to ensure only authorised personnel have access?		0%
	A.11.1.3	Securing offices, rooms and facilities	1. Have offices, rooms and facilities been designed and configured with security in mind? 2. Do processes for maintaining the security (e.g. Locking up, clear desks etc.) exist?		0%
	A.11.1.4	Protecting against external and environmental threats	Have physical protection measures to prevent natural disasters, malicious attack or accidents been designed in?		0%
	A.11.1.5	Working in secure areas	1. Do secure areas exist? 2. Where they do exist, do secure areas have suitable policies and processes? 3. Are the policies and processes enforced and monitored?		0%
	A.11.1.6	Delivery and loading areas	1. Are there separate delivery / loading areas? 2. Is access to these areas controls? 3. Is access from loading areas isolated from information processing facilities?		0%
	A.11.2	**Equipment**			

	A.11.2.1	Equipment siting and protection	1. Are environmental hazards identified and considered when equipment locations are selected? 2. Are the risks from unauthorised access / passers-by considered when siting equipment?		0%
	A.11.2.2	Supporting utilities	1. Is there a UPS system or back up generator? 2. Have these been tested within an appropriate timescale?		0%
	A.11.2.3	Cabling security	1. Have risk assessments been conducted over the location of power and telecommunications cables? 2. Are they located to protect from interference, interception or damage?		0%
	A.11.2.4	Equipment maintenance	Is there a rigorous equipment maintenance schedule?		0%
	A.11.2.5	Removal of assets	1. Is there a process controlling how assets are removed from site? 2. Is this process enforced? 3. Are spot checks carried out?		0%
	A.11.2.6	Security of equipment and assets off-premises	1. Is there a policy covering security of assets off-site? 2. Is this policy widely communicated?		0%
	A.11.2.7	Secure disposal or reuse of equipment	1. Is there a policy covering how information assets may be reused? 2. Where data is wiped, is this properly verified before reuse/disposal?		0%
	A.11.2.8	Unattended user equipment	1. Does the organisation have a policy around how unattended equipment should be protected? 2. Are technical controls in place to secure equipment that has been inadvertently left unattended?		0%
	A.11.2.9	Clear desk and clear screen policy	1. Is there a clear desk / clear screen policy? 2. Is this well enforced?		0%
	A.12	**Operations security**			
	A.12.1	**Operational procedures and responsibilities**			
	A.12.1.1	Documented operating procedures	1. Are operating procedures well documented? 2. Are the procedures made available to all users who need them?		0%
	A.12.1.2	Change management	Is there a controlled change management process in place?		0%
	A.12.1.3	Capacity management	Is there a capacity management process in place?		0%
	A.12.1.4	Separation of development, testing and operational environments	Does the organisation enforce segregation of development, test and operational environments?		0%
	A.12.2	**Protection from malware**			
	A.12.2.1	Controls against malware	1. Are processes to detect malware in place? 2. Are processes to prevent malware spreading in place? 3. Does the organisation have a process and capacity to recover from a malware infection.		0%
	A.12.3	**Backup**			

	A.12.3.1	Information backup	1. Is there an agreed backup policy? 2. Does the organisation's backup policy comply with relevant legal frameworks? 3. Are backups made in accordance with the policy? 4. Are backups tested?		0%
	A.12.4	**Logging and monitoring**			
	A.12.4.1	Event logging	Are appropriate event logs maintained and regularly reviewed?		0%
	A.12.4.2	Protection of log information	Are logging facilities protected against tampering and unauthorised access?		0%
	A.12.4.3	Administrator and operator logs	Are sysadmin / sysop logs maintained, protected and regularly reviewed?		0%
	A.12.4.4	Clock synchronisation	Are all clocks within the organisation		0%
	A.12.5	**Control of operational software**			
	A.12.5.1	Installation of software on operational systems	Is there a process in place to control the installation of software onto operational systems?		0%
	A.12.6	**Technical vulnerability management**			
	A.12.6.1	Management of technical vulnerabilities	1. Does the organisation have access to updated and timely information on technical vulnerabilities? 2. Is there a process to risk assess and react to any new vulnerabilities as they are discovered?		0%
	A.12.6.2	Restrictions on soft-ware installation	Are there processes in place to restrict how users install software?		0%
	A.12.7	**Information systems audit considerations**			
	A.12.7.1	Information systems audit controls	1. Are IS Systems subject to audit? 2. Does the audit process ensure business disruption is minimised?		0%
	A.13	**Communications security**			
	A.13.1	**Network security management**			
	A.13.1.1	Network controls	Is there a network management process in place?		0%
	A.13.1.2	Security of network services	1. Does the organisation implement a risk management approach which identifies all network services and service agreements? 2. Is security mandated in agreements and contracts with service providers (in house and outsourced). 3. Are security related SLAs mandated?		0%
	A.13.1.3	Segregation in networks	Does the network topology enforce segregation of networks for different tasks?		0%
	A.13.2	**Information transfer**			
	A.13.2.1	Information transfer policies and procedures	1. Do organisational policies govern how information is transferred? 2. Are procedures for how data should be transferred made available to all employees? 3. Are relevant technical controls in place to prevent non-authorised forms of data transfer?		0%
	A.13.2.2	Agreements on information transfer	Do contracts with external parties and agreements within the organisation detail the requirements for securing business information in transfer?		0%
	A.13.2.3	Electronic messaging	Do security policies cover the use of information transfer while using electronic messaging systems?		0%

	A.13.2.4	Confidentiality or nondisclosure agreements	1. Do employees, contractors and agents sign confidentiality or non disclosure agreements? 2. Are these agreements subject to regular review? 3. Are records of the agreements maintained?		0%
	A.14	**System acquisition, development and maintenance**			
	A.14.1	**Security requirements of information systems**			
	A.14.1.1	Information security requirements analysis and specification	1. Are information security requirements specified when new systems are introduced? 2. When systems are being enhanced or upgraded, are security requirements specified and addressed?		0%
	A.14.1.2	Securing application services on public networks	Do applications which send information over public networks appropriately protect the information against fraudulent activity, contract dispute, unauthorised discloser and unauthorised modification?		0%
	A.14.1.3	Protecting application services transactions	Are controls in place to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay attacks?		0%
	A.14.2	**Security in development and support processes**			
	A.14.2.1	Secure development policy	1. Does the organisation develop software or systems? 2. If so, are there policies mandating the implementation and assessment of security controls?		0%
	A.14.2.2	System change control procedures	Is there a formal change control process?		0%
	A.14.2.3	Technical review of applications after operating platform changes	Is there a process to ensure a technical review is carried out when operating platforms are changed?		0%
	A.14.2.4	Restrictions on changes to software packages	Is there a policy in place which mandates when and how software packages can be changed or modified?		0%
	A.14.2.5	Secure system engineering principles	Does the organisation have documented principles on how systems must be engineered to ensure security?		0%
	A.14.2.6	Secure development environment	1. Has a secure development environment been established? 2. Do all projects utilise the secure development environment appropriately during the system development lifecycle?		0%
	A.14.2.7	Outsourced development	1. Where development has been outsourced is this supervised? 2. Is externally developed code subject to a security review before deployment?		0%
	A.14.2.8	System security testing	Where systems or applications are developed, are they security tested as part of the development process?		0%
	A.14.2.9	System acceptance testing	Is there an established process to accept new systems / applications, or upgrades, into production use?		0%
	A.14.3	**Test data**			
	A.14.3.1	Protection of test data	1. Is there a process for selecting test data? 2. Is test data suitably protected?		0%
	A.15	**Supplier relationships**			
	A.15.1	**Information security in supplier relationships**			

	A.15.1.1	Information security policy for supplier relationships	1. Is information security included in contracts established with suppliers and service providers? 2. Is there an organisation-wide risk management approach to supplier relationships?		0%
	A.15.1.2	Addressing security within supplier agreements	1. Are suppliers provided with documented security requirements? 2. Is supplier access to information assets & infrastructure controlled and monitored?		0%
	A.15.1.3	Information and communication technology supply chain	Do supplier agreements include requirements to address information security within the service & product supply chain?		0%
	A.15.2	**Supplier service delivery management**			
	A.15.2.1	Monitoring and review of supplier services	Are suppliers subject to regular review and audit?		0%
	A.15.2.2	Managing changes to supplier services	Are changes to the provision of services subject to a management process which includes security & risk assessment?		0%
	A.16	**Information security incident management**			
	A.16.1	**Management of information security incidents and improvements**			
	A.16.1.1	Responsibilities and procedures	Are management responsibilities clearly identified and documented in the incident management processes?		0%
	A.16.1.2	Reporting information security events	1. Is there a process for timely reporting of information security events? 2. Is there a process for reviewing and acting on reported information security events?		0%
	A.16.1.3	Reporting information security weaknesses	1. Is there a process for reporting of identified information security weaknesses? 2. Is this process widely communicated? 3. Is there a process for reviewing and addressing reports in a timely manner?		0%
	A.16.1.4	Assessment of and decision on information security events	Is there a process to ensure information security events are properly assessed and classified?		0%
	A.16.1.5	Response to information security incidents	Is there an incident response process which reflects the classification and severity of information security incidents?		0%
	A.16.1.6	Learning from information security incidents	Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events?		0%
	A.16.1.7	Collection of evidence	1. Is there a forensic readiness policy? 2. In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence?		0%
	A.17	**Information security aspects of business continuity management**			
	A.17.1	**Information security continuity**			
	A.17.1.1	Planning information security continuity	Is information security included in the organisation's continuity plans?		0%
	A.17.1.2	Implementing information security continuity	Does the organisation's information security function have documented, implemented and maintained processes to maintain continuity of service during an adverse situation?		0%

	A.17.1.3	Verify, review and evaluate information security continuity	Are continuity plans validated and verified at regular intervals?		0%
	A.17.2	**Redundancies**			
	A.17.2.1	Availability of information processing facilities	Do information processing facilities have sufficient redundancy to meet the organisations availability requirements?		0%
	A.18	**Compliance**			
	A.18.1	**Compliance with legal and contractual requirements**			
	A.18.1.1	Identification of applicable legislation and contractual requirements	1. Has the organisation identified and documented all relevant legislative, regulatory or contractual requirements related to security? 2. Is compliance documented?		0%
	A.18.1.2	Intellectual property rights	1. Does the organisation keep a record of all intellectual property rights and use of proprietary software products? 2. Does the organisation monitor for the use of unlicensed software?		0%
	A.18.1.3	Protection of records	Are records protected from loss, destruction, falsification and unauthorised access or release in accordance with legislative, regulatory, contractual and business requirements?		0%
	A.18.1.4	Privacy and protection of personally identifiable information	1. Is personal data identified and appropriately classified? 2. Is personal data protected in accordance with relevant legislation?		0%
	A.18.1.5	Regulation of cryptographic controls	Are cryptographic controls protected in accordance with all relevant agreements, legislation and regulations?		0%
	A.18.2	**Information security reviews**			
	A.18.2.1	Independent review of information security	1. Is the organisations approach to managing information security subject to regular independent review? 2. Is the implementation of security controls subject to regular independent review?		0%
	A.18.2.2	Compliance with security policies and standards	1. Does the organisation instruct managers to regularly review compliance with policy and procedures within their area of responsibility? 2. Are records of these reviews maintained?		0%
	A.18.2.3	Technical compliance review	Does the organisation regularly conduct technical compliance reviews of its information systems?		0%