SUSTAINABLE Certification™

Our focus is your progress

SCPL ISO/IEC 27001:2022 Information Security Management Systems

Pre-Assessment Checklist

JAS-ANZ

SUSTAINABLE CERTIFICATION ISO 27001

4	Context of the organisation	
4.1	**Understanding the organisation and its context** The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. NOTE - Determining these issues refers to establishing the external and internal context of the organisation considered in Clause 5.4.1 of ISO 31000:2018.	

4.2	**Understanding the needs and expectations of interested parties** The organisation shall determine: a) interested parties that are relevant to the information security management system; b) the relevant requirements of these interested parties; c) which of these requirements will be addressed through the information security management system. NOTE - The requirements of interested parties can include legal and regulatory requirements and contractual obligations.	

4.3	**Determining the scope of the information security management system** The organisation shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organisation shall consider: a) the external and internal issues referred to in 4.2 b) the requirements referred to in 4.2	

	c) interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations. Is the Scope available as documented information?	

4.4	**Information security management system** Has the organisation demonstrated continual improvement of their ISMS? Has the organisation ensured sequence of processes and interactions?	

5	**Leadership**	
5.1	**Leadership and commitment** Has Top management demonstrated leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organisation; b) ensuring the integration of the information security management system requirements into the organisation's processes; c) ensuring that the resources needed for the information security management system are available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the	

	information securitymanagement system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility. NOTE - Reference to “business” in this document can be interpreted broadly to mean those activities that are core to the purposes of the organisation’s existence.	

5.2	**Policy** Has Top management established an information security policy that: a) is appropriate to the purpose of the organisation; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; f) be communicated within the organisation; g) be available to interested parties, as appropriate.	

5.3	**Organisational roles, responsibilities and authorities** Does Top managementl ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organisation? Has Top management assigned the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this document;	

	b) reporting on the performance of the information security management system to top management. NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organisation.	

6	**Planning**	
6.1 6.1.1	General When planning for the information security management system, the organisation shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; c) achieve continual improvement. The organisation shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement the actions into its information security management systemprocesses; and 2) evaluate the effectiveness of these actions.	
6.1.2	Has the organisation defined and applied an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid and comparable	

	results; c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners; d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialise; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritise the analysed risks for risk treatment. Has the organisation shall retain documented information about the information security risk assessment process. Information security risk treatment Has the organisation defined and applied an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE 1 Organisations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that nonecessary controls have been omitted;	

	NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked. NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed. d) produce a Statement of Applicability that contains: — the necessary controls (see 6.1.3 b) and c)); — justification for their inclusion; — whether the necessary controls are implemented or not; and — the justification for excluding any of the Annex A controls. e) formulate an information security risk treatment plan; and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organisation shall retain documented information about the information security risk treatment process. NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].	

6.2	**Information security objectives and planning to achieve them** Has the organisation established information security objectives at relevant functions and levels. Are The information security objectives: a) consistent with the information security policy; b) measurable (if practicable);	

	c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be monitored; e) be communicated; f) be updated as appropriate; g) be available as documented information. The organisation shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organisation shall determine: what will be done; h) what resources will be required; i) who will be responsible; j) when it will be completed; and k) how the results will be evaluated.	

6.3	**Planning of changes** Has the organisation determined the need for changes to the information security management system? Are the changes carried out in a planned manner?	

7	**Support**	
7.1	**Resources** Has the organisation determined and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.	

7.2	**Competence** Has The organisation established the following: a) determine the necessary competence of person(s) doing work under its	

	control that affects itsinformation security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence. NOTE - Applicable actions can include, for example: the provision of training to, the mentoring of, or the re- assignment of current employees; or the hiring or contracting of competent persons.	

7.3	**Awareness** Is the Person doing work under the organisation's control aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management systemrequirements.	

7.4	**Communication** Does the organisation determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) how to communicate.	

7.5	**Documented information** General	
7.5.1	DoesThe organisation's information security management system include: a) documented information required by this document; and b) documented information determined by the organisation as being necessary for the effectivenessof the information security management system. NOTE The extent of documented information for an information security management system can differ from one organisation to another due to: 1) the size of organisation and its type of activities, processes, products and services; 2) the complexity of processes and their interactions; and 3) the competence of persons.	
	Creating and updating	
7.5.2	When creating and updating documented information does the organisation ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy.	
	Control of documented information	
7.5.3	Documented information required by the information security management system and by this document shall be controlled to ensure: a) it is available and suitable for use, where and when it is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of	

	integrity). For the control of documented information, the organisation shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. version control); and f) retention and disposition. Documented information of external origin, determined by the organisation to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled. NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.	

8	**Operation**	
8.1	**Operational planning and control** Does the organisation plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: — establishing criteria for the processes; — implementing control of the processes in accordance with the criteria. Is the Documented information available to the extent necessary to have confidence that the processes have been carried out as planned. The organisation shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organisation shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.	

8.2	**Information security risk assessment** The organisation shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). Does The organisation retain documented information of the results of the information security risk assessments?	

8.3	**Information security risk treatment** Does the organisation implement the information security risk treatment plan. The organisation shall retain documented information of the results of the information security risk treatment.	

9	**Performance evaluation**	
9.1	**Monitoring, measurement, analysis and evaluation** The organisation shall determine: a) what needs to be monitored and measured, including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid; c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analysed and evaluated; f) who shall analyse and evaluate these results. Documented information shall be available as	

	evidence of the results. The organisation shall evaluate the information security performance and the effectiveness of the information security management system.	

9.2	**Internal audit**	
9.2.1	General Has the organisation conducted internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organisation's own requirements for its information security management system; 2) the requirements of this document; b) is effectively implemented and maintained.	
9.2.2	Internal audit programme Has the organisation planned, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. When establishing the internal audit programme(s), the organisation shall consider the importance of the processes concerned and the results of previous audits. The organisation shall: a) define the audit criteria and scope for each audit; b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; c) ensure that the results of the audits are reported to relevant management; Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.	

9.3	**Management review**	
9.3.1	General Top management shall review the organisation's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.	
9.3.2	Management review inputs Does the management review include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) changes in needs and expectations of interested parties that are relevant to the information security management system; d) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; 4) fulfilment of information security objectives; e) feedback from interested parties; f) results of risk assessment and status of risk treatment plan; g) opportunities for continual improvement.	
9.3.3	Management review results The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. Documented information shall be available as evidence of the results of management reviews.	

10	Improvement	
10.1	**Continual improvement** HasThe organisation continually improved the suitability, adequacy and effectiveness of the information security management system.	

10.2	**Nonconformity and corrective action** When a nonconformity occurs, the organisation shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recuror occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of: f) the nature of the nonconformities and any subsequent actions taken, g) the results of any corrective action.	

Table A.1 – Information security controls

5	Organisational controls	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be de- fined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organisation needs.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
5.4	Management responsibilities	**Control** Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.
5.5	Contact with authorities	**Control** The organisation shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest groups	**Control** The organisation shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.7	Threat intelligence	**Control** Information relating to information security threats shall be collected and analysed to produce threat intelligence.
5.8	Information security in project management	**Control** Information security shall be integrated into project management.
5.9	Inventory of information and other associated assets	**Control** An inventory of information and other associated assets, including owners, shall be developed and maintained.
5.10	Acceptable use of information and other associated assets	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.

5.11	Return of assets	**Control** Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.
5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements.
5.13	Labelling of information	**Control** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.
5.14	Information transfer	**Control** Information transfer rules, procedures, or agreements shall be in placefor all types of transfer facilities within the organisation and between the organisation and other parties.
5.15	Access control	**Control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
5.16	Identity management	**Control** The full life cycle of identities shall be managed.
5.17	Authentication information	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
5.18	Access rights	**Control** Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.
5.19	Information security in supplierrelationships	**Control** Processes and procedures shall be defined and implemented to managethe information security risks associated with the use of supplier's products or services.

5.20	Addressing information security within supplier agreements	**Control** Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review and change management of supplier services	**Control** The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
5.23	Information security for use of cloud services	**Control** Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.
5.24	Information security incident management planning and preparation	**Control** The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
5.25	Assessment and decision on in-formation security events	**Control** The organisation shall assess information security events and decide if they are to be categorised as information security incidents.
5.26	Response to information security Incidents	**Control** Information security incidents shall be responded to in accordance with the documented procedures.
5.27	Learning from information security incidents	**Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
5.28	Collection of evidence	**Control** The organisation shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.
5.29	Information security during disruption	**Control** The organisation shall plan how to maintain information security at an appropriate level during disruption.

5.30	ICT readiness for business continuity	**Control** ICT readiness shall be planned, implemented, maintained and testedbased on business continuity objectives and ICT continuity requirements.
5.31	Legal, statutory, regulatory and contractual requirements	**Control** Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and kept up to date.
5.32	Intellectual property rights	**Control** The organisation shall implement appropriate procedures to protectintellectual property rights.
5.33	Protection of records	**Control** Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release.
5.34	Privacy and protection of personal identifiable information (PII)	**Control** The organisation shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicablelaws and regulations and contractual requirements.
5.35	Independent review of information security	**Control** The organisation's approach to managing information security anditsimplementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.
5.36	Compliance with policies, rules and standards for information security	**Control** Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.
5.37	Documented operating procedures	**Control** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.
6	**People controls**	
6.1	Screening	**Control** Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoingbasis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the

		classification of the information to be accessed and the perceived risks.
6.2	Terms and conditions of employment	**Control** The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security.
6.3	Information security awareness, education and training	**Control** Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.
6.4	Disciplinary process	**Control** A disciplinary process shall be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.
6.5	Responsibilities after termination or change of employment	**Control** Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.
6.6	Confidentiality or non-disclosure agreements	**Control** Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
6.7	Remote working	**Control** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.
6.8	Information security event re-porting	**Control** The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
7	**Physical controls**	
7.1	Physical security perimeters	**Control** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.

7.2	Physical entry	**Control** Secure areas shall be protected by appropriate entry controls and access points.
7.3	Securing offices, rooms and facilities	**Control** Physical security for offices, rooms and facilities shall be designed and implemented.
7.4	Physical security monitoring	**Control** Premises shall be continuously monitored for unauthorised physical access.
7.5	Protecting against physical and environmental threats	**Control** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
7.6	Working in secure areas	**Control** Security measures for working in secure areas shall be designed and implemented.
7.7	Clear desk and clear screen	**Control** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
7.8	Equipment siting and protection	**Control** Equipment shall be sited securely and protected.
7.9	Security of assets off-premises	**Control** Off-site assets shall be protected.
7.10	Storage media	**Control** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.
7.11	Supporting utilities	**Control** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.
7.12	Cabling security	**Control** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.

7.13	Equipment maintenance	**Control** Equipment shall be maintained correctly to ensure availability, integrity, and confidentiality of information.
7.14	Secure disposal or reuse of equipment	**Control** Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse.
8	**Technological controls**	
8.1	User end point devices	**Control** Information stored on, processed by or accessible via user end point devices shall be protected.
8.2	Privileged access rights	**Control** The allocation and use of privileged access rights shall be restricted and managed.
8.3	Information access restriction	**Control** Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.
8.4	Access to source code	**Control** Read and write access to source code, development tools and software libraries shall be appropriately managed.
8.5	Secure authentication	**Control** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
8.6	Capacity management	**Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
8.7	Protection against malware	**Control** Protection against malware shall be implemented and supported by appropriate user awareness.
8.8	Management of technical vulnerabilities	**Control** Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.
8.9	Configuration management	**Control**

		Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
8.10	Information deletion	**Control** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.
8.11	Data masking	**Control** Data masking shall be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.
8.12	Data leakage prevention	**Control** Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.
8.13	Information backup	**Control** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
8.14	Redundancy of information processing facilities	**Control** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
8.15	Logging	**Control** Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.
8.16	Monitoring activities	**Control** Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
8.17	Clock synchronisation	**Control** The clocks of information processing systems used by the organisation shall be synchronised to approved time sources.
8.18	Use of privileged utility programs	**Control** The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.

8.19	Installation of software on operational systems	**Control** Procedures and measures shall be implemented to securely manage software installation on operational systems.
8.20	Networks security	**Control** Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
8.21	Security of network services	**Control** Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.
8.22	Segregation of networks	**Control** Groups of information services, users and information systems shall be segregated in the organisation's networks.
8.23	Web filtering	**Control** Access to external websites shall be managed to reduce exposure to malicious content.
8.24	Use of cryptography	**Control** Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
8.25	Secure development life cycle	**Control** Rules for the secure development of software and systems shall be established and applied.
8.26	Application security requirements	**Control** Information security requirements shall be identified, specified and approved when developing or acquiring applications.
8.27	Secure system architecture and engineering principles	**Control** Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
8.29	Security testing in development and acceptance	**Control** Security testing processes shall be defined and implemented in the development life cycle.

8.30	Outsourced development	**Control** The organisation shall direct, monitor and review the activities related to outsourced system development.
8.31	Separation of development, test and production environments	**Control** Development, testing and production environments shall be separated and secured.
8.32	Change management	**Control** Changes to information processing facilities and information systems shall be subject to change management procedures.
8.33	Test information	**Control** Test information shall be appropriately selected, protected and managed.
8.34	Protection of information systems during audit testing	**Control** Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.