SSR2 Workplan: ICANNSecurity - Workplan

ID		Key Action Step	Action	Expected Outcome	Data Source / Evaluation Methodology	Skill [1]	Responsible	Timeline	Reference	Comment
1.0		**Gap Analysis Information Security Management System ISO 27001**	**Planning and performing a gap-analysis based on ISO 27001**	**Report with recommendations how to comply with ISO 27001**	*** Interview * Documentation Review * Site visit**	**AUD, ISM, RM**				
	1.1	Scoping	Read all relevant documentation of the organizational structure and talk with stakeholders to identify boundaries, external groups, etc. to define the scope of the audit.	Agreed ISMS audit scope.	* Interview * Documentation Review	AUD, ISM				
	1.2	Pre-Audit	Read all relevant documentation of the ISMS in order to become acquainted with the processes in the management system and to find out if there are non-conformities in the (mandatory) documentation with regard to ISO 27001	Base for creating a (customized) audit workplan/checklist in consideration of the Statement of Applicability.	* Interview * Documentation Review	AUD, ISM				
	1.3	Preparing for main audit	Collect and study previous audit findings and possible outstanding issues. * Prepare all relevant documents that will be needed for the realization of the audit. * Create a audit checklist (must be in-depth and based on ISO 27001, following a predefined path and checking for compliance with controls).	(Customized) audit workplan/checklist and an audit plan agreed with management.	* Interview * Documentation Review	AUD, ISM				
	1.4	Planning the main audit	* Plan which departments and/or locations to visit and which ressources are needed. * Ensure the availability of all the resources needed and other logistics that may be required by the auditor.	Detailed workplan with committited ressources.	* Interview * Documentation Review	AUD, ISM, RM				
	1.5	Performing the audit	Perform the audit and try to find adequate evidence to ascertain that: * The ISMS is compliant with ISO 27001 (further information in the following sheets - ref. checklist 27001, Annex A) * The information security policy is still an accurate reflection of the business requirements. * An appropriate risk assessment methodology is being used. * The documented procedures are being followed (i.e. within the scope of the ISMS) and are meeting their desired objectives. * Technical controls (e.g. firewalls, physical access controls) are in place, are correctly configured and working as intended. * The residual risks have been assessed correctly and are still acceptable to the management of the company.	Documented audit findings	* Interview * Documentation Review * Site visit	AUD, ISM, LG, RM				
	1.6	Reporting	Summarize all the (non)conformities and write an audit report	Report		AUD				
2.0		**Gap Analysis Business Continuity Management System ISO 22301**	**Planning and performing a gap-analysis based on ISO 22301**	**Report with recommendations how to comply with ISO 22301**	*** Interview * Documentation Review * Site visit**	**AUD, BCM, RM**				
	2.1	Scoping	Read all relevant documentation of the organizational structure and talk with stakeholders to identify boundaries, external groups, etc. to define the scope of the audit.	Agreed BCMS audit scope.	* Interview * Documentation Review	AUD, BCM				
	2.2	Pre-Audit	Read all relevant documentation of the BCMS in order to become acquainted with the processes in the management system and to find out if there are non-conformities in the (mandatory) documentation with regard to ISO 22301.	Base for creating a (customized) audit workplan/checklist in consideration of the Statement of Applicability.	* Interview * Documentation Review	AUD, BCM				

SSR2 Workplan: ICANNSecurity - Workplan

ID		Key Action Step	Action	Expected Outcome	Data Source / Evaluation Methodology	Skill [1]	Responsible	Timeline	Reference	Comment
	2.3	Preparing for main audit	Collect and study previous audit findings and possible outstanding issues. * Prepare all relevant documents that will be needed for the realization of the audit. * Create a audit checklist (must be in-depth and based on ISO 22301, following a predefined path and checking for compliance with controls).	(Customized) audit workplan/checklist and an audit plan agreed with management.	* Interview * Documentation Review	AUD, BCM				
	2.4	Planning the main audit	* Plan which departments and/or locations to visit and which ressources are needed. * Ensure the availability of all the resources needed and other logistics that may be required by the auditor.	Detailed workplan with committited ressources.	* Interview * Documentation Review	AUD, BCM				
	2.5	Performing the audit	Perform the audit and try to find adequate evidence to ascertain that the BCMS is compliant with ISO 22301 (further information in the following sheets - ref. check list) * The business continuity policy is still an accurate reflection of the business requirements. * An appropriate risk assessment methodology is being used. * The documented procedures are being followed (i.e. within the scope of the BCMS) and are meeting their desired objectives. * Technical controls are in place, are correctly configured and working as intended. * The residual risks have been assessed correctly and are still acceptable to the management of the company.	Documented audit findings	* Interview * Documentation Review * Site visit	AUD, BCM, LG, RM				
	2.6	Reporting	Summarize all the (non)conformities and write an audit report	Report		AUD				
3.0		**Scope of ICANN's SSR responsibilities [2]**	**Review and analyze ICANN's Scope of SSR resonsibilities**	**Report with recommendations**						
	3.1	ICANN action zone	Review and analyze the documentation and produce recommendations.	Report	* Interview * Documentation Review	AUD, ISM				
	3.2	ICANN influence zone	Review and analyze the documentation and produce recommendations.	Report	* Interview * Documentation Review	AUD, ISM				
	3.3	ICANN coordination zone	Review and analyze the documentation and produce recommendations.	Report	* Interview * Documentation Review	AUD, ISM				
4.0		**ICANN Compliance**								
	4.1	Registrars	Review and analyze the level of compliance requirements for registrar agreements.	Report with recommendations	* Interview * Documentation Review	AUD, LG				
	4.2	Registries	Review and analyze the level of compliance requirements for registry agreements.	Report with recommendations	* Interview * Documentation Review	AUD, LG				
	4.3	Vetting RO	Review and analyze ICANN's processes around vetting registry operators .	Report with recommendations	* Interview * Documentation Review	AUD, BCM, LG				
	4.4	Vetting EBERO	Review and analyze ICANN's processes around vetting (emergency backend) registry operators.	Report with recommendations	* Interview * Documentation Review	AUD, BCM, LG				
	4.5	Data Escrow Provider	Review and analye ICANN's processes around vetting data escrow provider.	Report with recommendations	* Interview * Documentation Review	AUD, BCM, LG				
5.0		**TBD**								

ID	Requirement of the standard ISO 27001 / 22301	Clause	Compliant Yes/No	Evidence	Comments
S.1	**Context of the Organization**	**4**			
S.1.1	Did the organization determine interested parties?	4.1			
S.1.2	Does the list of all of interested parties' requirements exist?	4.2			
S.1.3	Is the scope documented with clearly defined boundaries and interfaces?	4.3			
S.2	**Leadership**	**5**			
S.2.1	Are the general ISMS objectives compatible with the strategic direction?	5.1			
S.2.2	Does management ensure that ISMS achieves its objectives?	5.1			
S.2.3	Does Information Security Policy exist with objectives or framework for setting objectives?	5.2			
S.2.4	Is Information Security Policy communicated within the company?	5.2			
S.2.5	Are roles and responsibilities for information security assigned and communicated?	5.3			
S.3	**Planning - Risks and Opportunities**	**6**			
S.3.1	Is the risk assessment process documented, including the risk acceptance criteria and criteria for risk assessment?	6.1.2			
S.3.2	Are the risks identified, their owners, likelihood, consequences, and the level of risk; are these results documented?	6.1.2, 8.2			
S.3.3	Is the risk treatment process documented, including the risk treatment options?	6.1.3			
S.3.4	Are all the unacceptable risks treated using the options and controls from Annex A; are these results documented?	6.1.3, 8.3			
S.3.5	Is Statement of Applicability produced with justifications and status for each control?	6.3			
S.3.6	Does Risk treatment plan exist, approved by risk owners?	6.1.3, 8.3			
S.3.7	Does Risk treatment plan define who is responsible for implementation of which control, with which resources, what are the deadlines, and what is the evaluation method?	6.2			
S.4	**Support - Resources, Competence, Awareness & Communication**	**7**			
S.4.1	Are adequate resources provided for all the elements of ISMS?	7.1			

ID	Requirement of the standard ISO 27001 / 22301	Clause	Compliant Yes/No	Evidence	Comments
S.4.2	Are required competences defined, trainings performed, and records of competences maintained?	7.2			
S.4.3	Is the personnel aware of Information security policy, of their role, and consequences of not complying with the rules?	7.3			
S.4.4	Does the process for communication related to information security exist, including the responsibilities and what to communicate?	7.4			
S.4.5	Does the process for managing documents and records exist, including who reviews and approves documents, where and how they are published, stored and protected?	7.5			
S.4.6	Are documents of external origin controlled?	7.5			
S.5	**Operation**	**8**			
S.5.1	Are outsourced processes identified and controlled?	8.1			
S.6	**Performance Evaluation, Internal Audit, Management Review**	**9**			
S.6.1	Is it defined what needs to be measured, by which method, who is responsible, who will analyze and evaluate the results?	9.1			
S.6.2	Are the results of measurement documented and reported to responsible persons?	9.1			
S.6.3	Does an audit program exist that defines the timing, responsibilities, reporting, audit criteria and scope?	9.2			
S.6.4	Are internal audits performed according to audit program, results reported through the Internal audit report and relevant corrective actions raised?	9.2			
S.6.5	Is management review regularly performed, and are the results documented in minutes of the meeting?	9.3			
S.6.6	Did management decide on all the crucial issues important for the success of the ISMS?	9.3			
S.7	**Improvement**	**10**			
S.7.1	Does the organization react to every nonconformity?	10.1			

ID	Requirement of the standard ISO 27001 / 22301	Clause	Compliant Yes/No	Evidence	Comments
S.7.2	Does the organization consider eliminating the cause of nonconformity and, where appropriate, take corrective action?	10.1			
S.7.3	Are all nonconformities recorded, together with corrective actions?	10.1			
32 Questions					

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.1	**Information security policies**	**A.5**			
S.A.1.1	Are all necessary information security policies approved by management and published?	A.5.1.1			
S.A.1.2	Are all information security policies reviewed and updated?	A.5.1.2			
S.A.2	**Organization of information security**	**A.6**			
S.A.2.1	Are all information security responsibilities clearly defined through one or several documents?	A.6.1.1			
S.A.2.2	Are duties and responsibilities defined in such a way to avoid conflict of interest, particularly with the information and systems where high risks are involved?	A.6.1.2			
S.A.2.3	Is it clearly defined who should be in contact with which authorities?	A.6.1.3			
S.A.2.4	Is it clearly defined who should be in contact with special interest groups or professional associations?	A.6.1.4			
S.A.2.5	Are information security rules included in every project?	A.6.1.5			
S.A.2.6	Are there rules for secure handling of mobile devices?	A.6.2.1			
S.A.2.7	Are there rules defining how the company information is protected at teleworking sites?	A.6.2.2			
S.A.3	**Human resource security**	**A.7**			
S.A.3.1	Are background checks performed on candidates for employment or for contractors?	A.7.1.1			
S.A.3.2	Do the agreements with employees and contractors specify the information security responsibilities?	A.7.1.2			
S.A.3.3	Is management actively requiring all employees and contractors to comply with information security rules?	A.7.2.1			
S.A.3.4	Are all relevant employees and contractors being trained to perform their security duties, and do the awareness programs exist?	A.7.2.2			
S.A.3.5	Have all employees who have committed a security breach been subject to a formal disciplinary process?	A.7.2.3			
S.A.3.6	Are information security responsibilities that remain valid after the termination of employment defined in the agreement?	A.7.3.1			

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.4	**Asset Management**	**A.8**			
S.A.4.1	Is an Inventory of assets drawn up?	A.8.1.1			
S.A.4.2	Does every asset in Inventory of assets have a designated owner?	A.8.1.2			
S.A.4.3	Are the rules for appropriate handling of information and assets documented?	A.8.1.3			
S.A.4.4	Did all the employees and contractors return all the company assets when their employment was terminated?	A.8.1.4			
S.A.4.5	Is the information classified according to specified criteria?	A.8.2.1			
S.A.4.6	Is the classified information labeled according to the defined procedures?	A.8.2.2			
S.A.4.7	Are there procedures which define how to handle classified information?	A.8.2.3			
S.A.4.8	Are there the procedures which define how to handle removable media in line with the classification rules?	A.8.3.1			
S.A.4.9	Are there formal procedures for disposing of the media?	A.8.3.2			
S.A.4.10	Is the media that contains sensitive information protected during transportation?	A.8.3.3			
S.A.5	**Access Control**	**A.9**			
S.A.5.1	Is there an Access control policy which defines business and security requirements for access control?	A.9.1.1			
S.A.5.2	Do the users have access only to those networks and services they are specifically authorized for?	A.9.1.2			
S.A.5.3	Are access rights provided via a formal registration process?	A.9.2.1			
S.A.5.4	Is there a formal access control system when logging into information systems?	A.9.2.2			
S.A.5.5	Are privileged access rights managed with special care?	A.9.2.3			
S.A.5.6	Are initial passwords and other secret authentication information provided in a secure way?	A.9.2.4			
S.A.5.7	Do asset owners periodically check all the privileged access rights?	A.9.2.5			
S.A.5.8	Have the access rights to all employees and contractors been removed upon the termination of their contracts?	A.9.2.6			
S.A.5.9	Are there clear rules for users on how to protect passwords and other authentication information?	A.9.3.1			

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.5.10	Is the access to databases and applications restricted according to the Access control policy?	A.9.4.1			
S.A.5.11	Is secure log-on required on systems according to the Access control policy?	A.9.4.2			
S.A.5.12	Are the systems that manage passwords interactive, and enable the creation of secure passwords?	A.9.4.3			
S.A.5.13	Is the use of utility tools that can override the security controls of applications and systems strictly controlled and limited to narrow circle of employees?	A.9.4.4			
S.A.5.14	Is the access to source code restricted to authorized persons?	A.9.4.5			
S.A.6.0	**Cryptography**	**A.10**			
S.A.6.1	Does the policy that regulates encryption and other cryptographic controls exist?	A.10.1.1			
S.A.6.2	Are the cryptographic keys properly protected?	A.10.1.2			
S.A.7.0	**Physical and environmental security**	**A.11**			
S.A.7.1	Do secure areas that protect sensitive information exist?	A.11.1.1			
S.A.7.2	Is the entrance to secure areas protected with controls that allow only the authorized persons to enter?	A.11.1.2			
S.A.7.3	Are secure areas located in such a way that they are not visible to outsiders, and not easily reached from the outside?	A.11.1.3			
S.A.7.4	Are the alarms, fire-protection, and other systems installed?	A.11.1.4			
S.A.7.5	Are working procedures for secure areas defined and complied with?	A.11.1.5			
S.A.7.6	Are delivery and loading areas controlled in such a way that unauthorized persons cannot enter the company premises?	A.11.1.6			
S.A.7.7	Is the equipment sited in such a way to protect it from unauthorized access, and from environmental threats?	A.11.2.1			
S.A.7.8	Does the equipment have an uninterruptible power supply?	A.11.2.2			
S.A.7.9	Are the power and telecommunication cables adequately protected?	A.11.2.3			
S.A.7.10	Is the equipment maintained regularly according to manufacturers' specifications and good practice?	A.11.2.4			

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.7.11	Is the authorization for information and other assets given each time they are taken out of the company premises?	A.11.2.5			
S.A.7.12	Are the company assets adequately protected when they are not located at the company premises?	A.11.2.6			
S.A.7.13	Are all the information and licensed software removed from media or equipment containing media when disposed of?	A.11.2.7			
S.A.7.14	Are users protecting their equipment when not in physical possession of it?	A.11.2.8			
S.A.7.15	Is there a policy which forces users to remove papers and media when not present, and lock their screens?	A.11.2.9			
S.A.8.0	**Operations security**	**A.12**			
S.A.8.1	Have the operating procedures for IT processes been documented?	A.12.1.1			
S.A.8.2	Are all the changes to IT systems, but also to other processes that could affect information security, strictly controlled?	A.12.1.2			
S.A.8.3	Does someone monitor use of resources and project the required capacity?	A.12.1.3			
S.A.8.4	Are development, testing and production environments strictly separated?	A.12.1.4			
S.A.8.5	Are anti-virus software, and other software for malware protection, installed and updated?	A.12.2.1			
S.A.8.6	Is the backup policy developed; is the backup performed according to this policy?	A.12.3.1			
S.A.8.7	Are all user logs, faults and other events from IT systems logged, and does someone check them?	A.12.4.1			
S.A.8.8	Are logs protected in such a way that unauthorized persons cannot change them?	A.12.4.2			
S.A.8.9	Are administrator logs protected in such a way that system administrators cannot change them or delete them; are they regularly checked?	A.12.4.3			
S.A.8.10	Are clocks on all IT systems synchronized with a single source of correct time?	A.12.4.4			
S.A.8.11	Is installation of software strictly controlled; do procedures exist for that purpose?	A.12.5.1			

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.8.12	Is there someone in charge of collecting information about vulnerabilities, and are those vulnerabilities promptly resolved?	A.12.6.1			
S.A.8.13	Are there specific rules that define restrictions of software installation by users?	A.12.6.2			
S.A.8.14	Are audits of production systems planned and executed in such a way that they minimize the risk of disruption?	A.12.7.1			
S.A.9.0	**Communications security**	**A.13**			
S.A.9.1	Are the networks controlled in such a way that they protect information in systems and applications?	A.13.1.1			
S.A.9.2	Are security requirements for in-house and external network services defined, and included in agreements?	A.13.1.2			
S.A.9.3	Are groups of users, services and systems segregated in different networks?	A.13.1.3			
S.A.9.4	Is the protection of information transfer regulated in formal policies and procedures?	A.13.2.1			
S.A.9.5	Do agreements with third parties exist which regulate the security of information transfer?	A.13.2.2			
S.A.9.6	Are the messages that are exchanged over the networks properly protected?	A.13.2.3			
S.A.9.7	Did the company list all the confidentiality clauses that need to be included in agreements with third parties?	A.13.2.4			
S.A.10.0	**System acquisition, development and maintenance**	**A.14**			
S.A.10.1	Are security requirements defined for new information systems, or for any changes to them?	A.14.1.1			
S.A.10.2	Is the information involved in applications that is transferred through the public networks appropriately protected?	A.14.1.2			
S.A.10.3	Is the information involved in transactions that is transferred through the public networks appropriately protected?	A.14.1.3			
S.A.10.4	Are the rules for the secure development of software and systems defined?	A.14.2.1			

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.10.5	Do formal change control procedures exist for making any changes to the new or existing systems?	A.14.2.2			
S.A.10.6	Are critical applications tested after the operating systems have been changed or updated?	A.14.2.3			
S.A.10.7	Are only the changes that are really necessary performed to information systems?	A.14.2.4			
S.A.10.8	Are the principles for engineering secure systems documented and implemented?	A.14.2.5			
S.A.10.9	Is the development environment appropriately secured from unauthorized access and change?	A.14.2.6			
S.A.10.10	Is the outsourced development of systems monitored?	A.14.2.7			
S.A.10.11	Is testing for proper implementation of security requirements performed during the development?	A.14.2.8			
S.A.10.12	Are the criteria for accepting the systems defined?	A.14.2.9			
S.A.10.13	Are the test data carefully selected and protected?	A.14.3.1			
S.A.11.0	**Supplier relationships**	**A.15**			
S.A.11.1	Is the policy on how to treat the risks related to suppliers and partners documented?	A.15.1.1			
S.A.11.2	Are all the relevant security requirements included in the agreements with the suppliers and partners?	A.15.1.2			
S.A.11.3	Do the agreements with cloud providers and other suppliers include security requirements for ensuring the reliable delivery of services?	A.15.1.3			
S.A.11.4	Are suppliers regularly monitored for compliance with the security requirements, and audited if appropriate?	A.15.2.1			
S.A.11.5	When making changes to arrangements and contracts with suppliers and partners, are risks and existing processes taken into account?	A.15.2.2			
S.A.12.0	**Information security incident management**	**A.16**			
S.A.12.1	Are procedures and responsibilities for managing incidents clearly defined?	A.16.1.1			
S.A.12.2	Are all information security events reported in a timely manner?	A.16.1.2			
S.A.12.3	Are employees and contractors reporting on security weaknesses?	A.16.1.3			

ID	Requirement of the standard ISO/IEC 27001 - Annex A	Clause	Compliant Yes/No	Evidence	Comments
S.A.12.4	Are all security events assessed and classified?	A.16.1.4			
S.A.12.5	Are procedures on how to respond to incidents documented?	A.16.1.5			
S.A.12.6	Are security incidents analyzed in order to gain knowledge on how to prevent them?	A.16.1.6			
S.A.12.7	Do procedures exist which define how to collect evidence that will be acceptable during the legal process?	A.16.1.7			
S.A.13.0	**Information security aspects of business continuity management**	**A.17**			
S.A.13.1	Are requirements for continuity of information security defined?	A.17.1.1			
S.A.13.2	Do procedures exist that ensure the continuity of information security during a crisis or a disaster?	A.17.1.2			
S.A.13.3	Is exercising and testing performed in order to ensure effective response?	A.17.1.3			
S.A.13.4	Does IT infrastructure have redundancy (e.g. secondary location) to fulfill the expectations during disasters?	A.17.2.1			
S.A.14.0	**Compliance**	**A.18**			
S.A.14.1	Are all legislative, regulatory, contractual and other security requirements listed and documented?	A.18.1.1			
S.A.14.2	Do procedures exist that ensure the enforcement of intellectual property rights, in particular, the used of licensed software?	A.18.1.2			
S.A.14.3	Are all the records protected according to identified regulatory, contractual and other requirements?	A.18.1.3			
S.A.14.4	Is personally identifiable information protected as required in laws and regulations?	A.18.1.4			
S.A.14.5	Are cryptographic controls used as required in laws and regulations?	A.18.1.5			
S.A.14.6	Is information security regularly reviewed by an independent auditor?	A.18.2.1			
S.A.14.7	Do the managers regularly review if the security policies and procedures are performed properly in their areas of responsibility?	A.18.2.2			
S.A.14.8	Are information systems regularly reviewed to check their compliance with the information security policies and standards?	A.18.2.3			
114 Questions					

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.1	**Context of the Organization**	**4**			
B.1.1	**Understanding the Organization**				
B.1.1.1	Has the organization determined the external internal issues that are relevant to its purpose and affect its ability to achieve the intended outcomes of its BCMS?	4.1			
B.1.2	**Supply Chain**				
B.1.2.1	Does the organization have a documented Policy concerning the procurement, provision and management of outsourced good and services via its supply chain?	4.1			
B.1.3	**Understanding the Needs and Expectations of Interested Parties**				
B.1.3.1	Has the organization identified its stakeholders and interested parties that are relevant to the BCMS?	4.2.1			
B.1.4	**Legal and Regulatory Requirements**				
B.1.4.1	Does the organization have a process that identifies and applies its legal, regulatory, contractual and operating licence conditions that relate to the continuity of its operations, products, services and interests of relevant interested parties?	4.2.2			
B.1.5	**Business Continuity Management System (BCMS)**				
B.1.5.1	Has the organization determined and documented the scope of its BCMS?	4.3			
B.1.5.2	Has the organization established and implemented a Business Continuity Management System (BCMS)?	4.4			
B.1.6	**BCMS Assurance**				
B.1.6.1	Does the organization have a documented assurance process and programme for the BCMS and its component parts?	4.5			
B.1.6.2	Does the organization have set of key performance indicators (KPI's objectives, targets and standards) for the BCMS?	4.5			
B.1.6.3	Does the organization have a BCMS Management Information System (MIS) as a part of its overall management, monitoring and performance evaluation programme of the BCMS?	4.5			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.2	**Leadership and (Management) Commitment**	**5**			
B.2.1	Does the organization's top management and other relevant management roles throughout the organization demonstrate leadership, support and strong commitment with respect to the BCMS?	5.1			
B.2.2	Has the organization's top management established and published a documented organization business continuity policy?	5.3			
B.2.3	Has the organization's top management appointed one or more management representatives with the appropriate authority, competencies and capability to be responsible for the BCMS and to be accountable for its establishment, implementation , maintenance and effective operation?	5.4			
B.3	**Planning**	**6**			
B.3.1	**Actions to Address Risks and Opportunities**	6.1			
B.3.1.1	When planning for its BCMS does the organization consider the needs and expectations of interested parties that are relevant to its purpose and that affects its alility to achieve the intended outcomes of its BCMS?	6.1			
B.3.1.2	When planning for its BCMS does the organization consider the internal and external issues that are relevant to its purpose and that affects its ability to achieve the intended outcomes of its BCMS?	6.1			
B.3.1.3	When planning for the BCMS does the organization consider the risks and opportunites that are relevant to its purpose and that affects its alility to achieve the intended outcomes of its BCMS?	6.1			
B.3.2	**Business Continuity Objectives and Plans to achieve them**	6.2			
B.3.2.1	Does the organization have a plan for implementing and managing a BCMS (see Clause 8)?	6.2			
B.3.2.2	Has the organization's top management established its business continuity objectives?	6.2			
B.3.2.3	Does the organization's BCM objectives protect prioritised activities (products and services) their support resources and dependencies?	6.2			
B.4	**Support**	**7**			
B.4.1	**Resources**	7.1			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.4.1.1	Has the organization determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS?	7.1			
B.4.1.2	Has the organization nominated incident response personnel with the necessary responsibility, authority and competence to manage an incident?	7.1			
B.4.2	**Competence and Training**	7.2			
B.4.2.1	Does the organization ensure that all personnel and/or teams that have been assigned roles and responsibilities in the BCMS especially business continuity procedures and arrangements, are competent and capable of performing their roles?	7.2			
B.4.2.2	Has the organization established a training programme for all current employees that may be affected by and/or have to deal with a disruptive incident?	7.2			
B.4.3	**Awareness**	7.3			
B.4.3.1	Has the organization established a business continuity awareness programme for all current employees to promote and create awareness of the organization's BCMS?	7.3			
B.4.3.2	Has the organization established a process to build, promote, integrate and embed a business continity culture within the organization?	7.3			
B.4.4	**Communication**	7.4			
B.4.4.1	Has the organization established and implemented procedures for internal communication amongst interested parties and employees within the organization?	7.4			
B.4.4.2	Has the organization established and implemented procedures for external communication with customers, partners, local community and other interested parties including the media?	7.4			
B.4.5	**Documented Information**	7.5			
B.4.5.1	Does the organization control documentation to ensure it creates, maintains and protects documents in a manner that is approprite and sufficient to implement and operate its BCMS?	7.5.1			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.4.6	**Creating and Updating**	7.5.2			
B.4.6.1	When creating and updating documented information does the organization ensure appropriate identification and description, format, review and approval of suitability and adequacy?	7.5.2			
B.4.7	**Control of Documented Information**	7.5.3			
B.4.7.1	Can the control of documented information process be described as a complex document control system rather than its primary focus and purpose as described in clause 7.5.3 of ISO	7.5.3			
B.5	**OPERATION**	**8**			
B.5.1	**Operational planning and control**	8.1			
B.5.1.1	Does the organization have a documented business continuity operational planning and control process that enables it to determine, plan, implement and control those actions needed to fulfil its business continuity policy and objectives?	8.1			
B.5.2		8.2			
B.5.2.1	Does the organization have a formal documented standard procedure and evaluation process for conducting a BIA?	8.2.1			
B.5.2.2	Has the organization carried out a BIA to identify its prioritised activities?	8.2.1			
B.5.2.3	Have the financial and non-financial impacts and/or consequences of an incident or disruption, overtime, of not performing each of the organization's prioritised activities and/or their support and/or dependencies been identified and assessed?	8.2.1			
B.5.2.4	Have the Recovery Time Objective (RTO) for each prioritised activity been identified and agreed?	8.2.1			
B.5.2.5	Has the organization identified the dependencies and resources needed to maintain, restore, resume and/or recover each of its prioritised activities to an acceptable level of functionality and performance (MBCO)?	8.2.1			
B.5.3	**Risk assessment**	4.2.2			
B.5.3.1	Does the organization have a formal documented standardised procedure and process for carrying out risk assessment?	4.2.2			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.5.3.2	Is scenario planning used as a part of the risk assessment and management process in respect of the organization's prioritised activities their support resources and dependencies?	4.2.2			
B.5.3.3	Is there a procedure and process for an ongoing review of the disruptive incident related risks that have been identified in respect of the organization's prioritised activities their support resources and dependencies?	4.2.2			
B.5.4	**Business Continuity Strategies**	8.3			
B.5.4.1	Is there a documented Corporate (organization) BCM Strategy that has been signed-off by top management?	8.3.1			
B.5.5	**Prioritised Activity Recovery Strategy**	8.3.2			
B.5.5.1	Is there a documented Business Continuity Resumption/Recovery Strategy(ies) for the organization's prioritised activities their support resources and dependencies that has been signed off by top management?	8.3.2			
B.5.6	**Resource Recovery Strategy**	8.3.3			
B.5.6.1	Is there a documented Resource Recovery Strategy for critical business activities and their dependencies that has been signed off by top management?	8.3.3			
B.5.6.2	Is the strategy based upon and consistent with the resource recovery requirements identified within the current BIA in respect of the organization's prioritised activities their support services and dependencies recovery profile?	8.3.3			
B.5.6.3	Have the resource requirements to implement the business continuity strategies been identified and provided?	8.3.3			
B.5.7	**Establish and Implement BC Procedures - Incident Response Structure**	8.4			
B.5.7.1	Does each organization site and/or building have an Emergency Management/Evacuation Plan e.g. fire/bomb?	8.4.2			
B.5.7.2	Does the organization have an incident management structure, procedures and arrangements that provide overall control of the response to a disruptive incident?	8.4.2			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.5.7.3	Does the organization have a documented Corporate Crisis Management Plan (CCMP)?	8.4.2			
B.5.7.4	Does each plan provide a clearly defined process for dealing with internal and external communications, the media and public relations during an incident?	8.4.2			
B.5.7.5	Does each key site, building, business division and support function e.g. IT, have an Incident Management Plan?	8.4.2			
B.5.7.6	Is each plan and its component parts exercised at least once every 12 months?	8.4.2			
B.5.7.7	Is there a process to provide a prioritised and documented action plan(s) to implement approved changes to the plan within an agreed timescale e.g. post maintenance, audit, non-conformance, test reports or invocation of plans etc?	8.4.2			
B.5.7.8	Is there an incident notification, invocation (activation) and escalation process set out within each plan?	8.4.2			
B.5.7.9	Does each plan provide a clearly defined process for dealing with internal and external communications, the media and public relations during an incident?	8.4.2			
B.5.7.10	Are there predefined on-site and offsite Incident Management (Command and Co-ordination) Centre locations set out within each plan to manage a disruptive incident or corporate crisis?	8.4.2			
B.5.7.11	Does the organization's incident management include liaison with other organizations such as the emergency services, suppliers, regulators and other stakeholders/interested parties that may be involved in the management of a disruptive incident?	8.4.2			
B.5.7.12	Does the organization have predefined Incident Management Team(s) for co-ordinating and/or managing differing types of incident e.g. business, technical service delivery, site, building, corporate?	8.4.2			
B.5.7.13	Does each plan contain details of key tasks and actions that need to be carried out?	8.4.2			
B.5.7.14	Is there a documented and funded maintenance cycle and programme for each incident management plan and its component parts to ensure it remains appropriate (fit for purpose), plausible and capable of achieving its objectives and outcomes?	8.4.2			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.5.8.	**Warning and Communication**	8.4.3			
B.5.8.1	Does the organization incident response and business continuity structure provide for internal and external communication with interested parties including authorities and the media during an incident?	8.4.3			
B.5.8.2	Has the strategy and plan been successfully exercised and/or invoked at least once within the last 12 (twelve) months to ensure it can achieve its aim and objectives within the required timescales?	8.4.3			
B.5.8.3	Is there a structured and detailed notification, invocation (activation) and escalation process set out within the plan?	8.4.3			
B.5.8.4	Does the plan contain mandatory instructions, advice, process, procedure or guidelines concerning central co-ordination of internal and external communications and release of information?	8.4.3			
B.5.8.5	Does the organization have proven procedures and capability for special arrangements for issuing warnings, alerts and external communication rapidly especially to interested parties with special needs?	8.4.3			
B.5.8.6	Has the organization established a suitable venue to support the liaison with the media and other groups of interested parties?	8.4.3			
B.5.8.7	Does the organization have a press briefing facility (different from liaison facility)?	8.4.3			
B.5.8.8	Is there a documented and funded maintenance cycle and programme for the plan and its component parts to ensure it remains current, appropriate (fit for purpose), plausible and capable of meeting its objectives and outcomes?	8.4.3			
B.5.8.9	Does the organization have a Communications, Media and Public Relations (PR) Team?	8.4.3			
B.5.9	**Business Continuity Plans (BCP)**	8.4.4			
B.5.9.1	Does the organization have documented business continuity plans in respect of each of the organization's prioritised activities and their dependencies?	8.4.4			
B.5.9.2	Is each plan integrated with the organization's other business continuity plans and arrangements e.g. ITDR, work area recovery, media and public relations, incident and corporate crisis management?	8.4.4			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.5.9.3	Does each plan contain documented procedures and details of how each prioritised activity and its dependencies within the scope of the plan will be resumed and recovered? (ISO 22313 Clause 8.4.4.3.5)	8.4.4			
B.5.9.4	Does each plan identify roles and teams that have the necessary seniority, authority, capability and competence to take control and manage the incident and communicate with stakeholders?	8.4.4			
B.5.9.5	Does each plan contain nominated person(s) to manage the communications aspect of a business disruption?	8.4.4			
B.5.9.6	Does each plan contain details and identify the ICT systems on which their resumption relies and reference any ICT continuity procedures that exist? (ISO 22313 Clause 8.4.4.3.6) (further guidance on this area can be found in ISO 27301).	8.4.4			
B.5.9.7	Does each plan clearly identify, prioritise and document the non-technical e.g. personnel and work area recovery, resource recovery requirements for each prioritised activity?	8.4.4			
B.5.9.8	Has each plan and its component parts been successfully tested and/or invoked at least once within the last 12 months to ensure they can achieve its aim and objectives within the required timescales?	8.4.4			
B.5.9.9	Is there a detailed plan notification, invocation (activation) and escalation process set out within the plan?	8.4.4			
B.5.9.10	Is there a documented and funded maintenance cycle and programme for the plan and its component parts to ensure it remains appropriate (fit for purpose), plausible and capable of meeting its objectives and required outcomes?	8.4.4			
B.5.9.11	Does each plan contain predefined task checklists that includes mandatory and discretionary tasks together with individuals/roles/teams responsible for their completion and a process for tracking there completion within an allocated timeframe ?	8.4.4			
B.5.9.12	Are their internal and/or external contracts and/or service level agreements for BCM arrangements i.e. the provision of specialist services, resources and/or products?	8.4.4			
B.5.9.13	Is the level of specialist BCM service(s) clearly identified within the service contract and/or SLA, and a copy placed in the plan?	8.4.4			
B.5.9.14	Does the organization have safety and welfare procedures documented within each business continuity plan?	8.4.4			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.5.10	**Exercising and Testing**	8.5			
	Does the organization have a documented exercise/testing programme and process for business continuity procedures, plans and arrangements?	8.5			
B.6	**PERFORMANCE EVALUATION**	**9**			
B.6.1	Monitoring, Measurement, Analysis and Evaluation	9.1			
B.6.1.1	Does the organization evaluate the performance and effectiveness of its BCMS?	9.1.1			
B.6.2	**Evaluation of Business Continuity Procedures**	9.1.2			
B.6.2.1	Does the organization conduct performance evaluations of its business continuity procedures, arrangements and capabilities in order to verify their continued suitability, adequacy and effectiveness?	9.1.2			
B.6.2.2	Is a post incident review undertaken in the event of an incident that disrupts the organization's prioritised activities or requires an incident response?	9.1.2			
B.6.3	**BCMS Maintenance**	9.1.2			
B.6.3.1	Has the organization a clearly defined and documented maintenance programme for its BCMS including its business continuity procedures and arrangements in particular?				
B.6.4	**Internal Audit**	9.2			
B.6.4.1	Does the organization conduct internal audits at planned intervals to provide information on whether the BCMS is effectively implemented and maintained?	9.2			
B.6.5	**Management Review**	9.3			
B.6.5.1	Does top management review the performance of the organization's BCMS to ensure its continued suitability, adequacy and effectiveness?	9.3			
B.6.5.2	Does the review programme specify a report shall be produced after each management review?	9.3			
B.7	**IMPROVEMENT**	**10**			

ID	Requirement of the standard ISO 22301	Clause	Compliant Yes/No	Evidence	Comments
B.7.1	**Nonconformity and Corrective Action**	10.1			
B.7.1.1	When the organization identifes a nonconformity does it react to it and take action to control and correct it and deal with the consequences?	10.1			
B.7.2	**Continual Improvement**	10.2			
B.7.2.1	Does the organization continually improve the suitability, adequacy or effectiveness of the BCMS?	10.2			

Notes

[1] Skillset
Information Security Management (ISM), Audit (AUD), Risk Management (RM), Business Continuity Management (BCM), Legal (LG)

[2] Zarko Kecic:
Looks as joint effort of all subtopic groups.