Information on using the checklist

The presentcheck list is intended to list the requirements of the ISO 27001: 2017 standard, in their more general formulation, to allow the organization to verify and understand if the information security management system is structured, maintained and improved according to the requirements regulatory.

The points on the check list concern the higher structure of the standard, the one called High Level Structure (HLS). The attention paid to the higher structure of the standard is justified by the opportunity to ensure the possibility of integrating this information security management system with other ISO systems based on the same structure such as:

- The quality management system (ISO 9001)
- The environmental management system (ISO 14001)
- The management system for occupational safety (ISO 45001)
- The management system for the prevention of corruption (ISO 37001)
- The technological innovation management system (ISO 56002)

The HLS, foras far as possible, it allows an appreciable compatibility also with the systems that manage the requirements relating to the prevention of predicate offenses envisaged by Legislative Decree 231/01, for which the organization "protects" itself from administrative liability. Even systems that manage privacy in light of the new European regulation 679/2016 (GDPR) usually appreciate the application of this structure.

Any checklists that deepen theverification of compliance with the requirements belonging to an underlying level of the standard structure are drawn up, in relation to the requirements of the audit plan, by the Internal Auditor and indicated in the plan.

POINT	CHECKS	NC	DESCRIPTION
6.2	▪ They were established the objectives for the safety of information? ▪ Such are objectives consistent with the policy? ▪ The planning for the achievementthe security objectives of the information?	□	
7.1	▪ The organization has determinedand made available the resources needed to system operation management?	□	
7.2	▪ The organization selects people in relation to skills needed to operate the system of management? ▪ The organization provides for the related training activities the necessary skills?	□	
7.3	▪ The people who work in the organization are aware of the security policy of information? ▪ They are aware how they can contribute to the pursuit of the strategic objective (purpose strategic) of management system? ▪ They are aware the consequences of any non compliance?	□	
7.4	▪ The organization regulated internal communication and external with regard to the contents of the management	□	
7.5	▪ The organization has developed adocument system coherent? ▪ The ways in which the documents are created and updated? ▪ The information documented documents of the system are managed in in such a way as to allow efficient operation of the system?	□	
8.1	▪ The organization hasestablished and documented the processes that allow to to keep information safe? ▪ The organization hasestablished the manner in which the procedures that govern the processes are adapted to changes of the context?	□	

Information on using the checklist

This checklist reports, in accordance withaccording to Annex A of the ISO 27001: 2017 standard, the controls required for information security used by the organization.

In relation to each control there is the identification number which corresponds to the control number established by Annex A, the title and the related description. During the audit, each control indicated in annex MOD-610-B - Information security plan, and reported in the present checklist, must be verified in its effective and effective implementation.

In the absence of its application or in the presence of obvious application malfunctions that make its use not fully effective, the organization reports the non-compliance and describes it briefly so that it is reported in the audit documents and in those relating to the management of non-compliance.

The purposeof the check list is in fact to build a compliance grid to be used quickly and synoptic to ensure that no control required by the standard (Annex A) and deemed applicable is not neglected from the organization

	INFORMATION SECURITY POLICY			
POINT	CATEGORY	CHECKS	NC	DESCRIPTION OF THE NON-CONFORMITY
5.1.1	Policy for the security of information	Aset of security policies information must be defined, approvedby management, published e press releaseto staff and parties relevant external.	□	
5.1.2	Review of policies for the security of information	Thesecurity policies of information mustbe reviewed at scheduled intervals or if so significant changes have occurred, in order to always guarantee their suitability, the adequacy and effectiveness.	□	

7	HUMAN RESOURCES SAFETY			
POINT	CATEGORY	CHECKS	NC	DESCRIPTION OF THE NON-CONFORMITY
7.1.1	Screening	They have tochecks to be carried out for the background check on all job candidates in agreementwith the read, withrelevant regulations and with ethics and must be proportionate to business needs, to classification of the information to be accessed and the risks perceived	□	
7.1.2	TermsAnd conditions of use	The agreementscontractual with the staff e withcollaborators must specify the their responsibility and that of the organization in relation tosecurity of information.	□	
7.2.1	Responsibility management	The directionmust take all of the personaland collaborators to apply thereinformation security in compliance with thepolicies and proceduresestablished by the	□	
7.2.2	Awareness, instruction, formationAnd training security from the information	All staff of the organizationAnd, when relevant,collaborators, they must receiveadequate awareness raising, education, training and training and updates periodicalson policies and procedures organizational, sopertinent to their work activity.	□	
7.2.3	Process disciplinary	A process must be established disciplinary, formaland communicated, for take action in towards the personnel it has committed a security breach information	□	
7.3.1	Terminationor variation of responsibility during the Relationship of work	Theresponsibilities and duties related to information security that remainvalid after termination or change in the employment relationship must be defined, communicated to staff or to the collaborator and made effective.	□	

APPLICATION OF SECURITY CHECKS (ANNEX A 27001: 2017)

CHECKLIST 02

8	ASSET MANAGEMENT			
POINT	CATEGORY	CHECKS	NC	DESCRIPTION OF THE NON-CONFORMITY
8.1.1	Inventory of asset	All the assets associated with the information e to the processing facilities of the informationthey must be identified; a inventory of these assets must be compiledand kept up to date	☐	
8.1.2	Responsibility of the asset	Assets registered in the inventory must have a manager	☐	
8.1.3	Usage acceptableof the asset	Therules for the acceptable use of information and the assets associated with structures of information processing must be identified, documented and implemented.	☐	
8.1.4	Return of the asset	All the personnel and users of external parties they must all return the assets of the organization in their possession to term of period of employment, del contractor the agreement entered into	☐	
8.2.1	Classification from the information	The information must be classified in relation to their value, the mandatory requirements e criticality in case of disclosure o unauthorized modification	☐	
8.2.2	Labeling from the information	It has to be developedand implemented a appropriateset of procedures for labelinginformation based on the scheme of classification adopted from the organization	☐	
8.2.3	Treatment of the asset	It has to be developedand implemented a whole from procedures for the treatment of assets in baseto the adopted classification scheme from the organization	☐	
8.3.1	Managemen t of supports removable	Procedures for the treatment of removable media in base to the adopted classification scheme from the organization	☐	
8.3.2	Disposal of the supports	Theredisposal of supports no longer needed it must be done safely, through the use of formal procedures	☐	
8.3.3.	Transport of supports physical	Media that contain information they must be protected from non-accesses authorized, improper use or tampering during the transport	☐	

APPLICATION OF SECURITY CHECKS (ANNEX A 27001: 2017)

CHECK LIST-02

9	CONTROL OFACCESSES			
POINT	CATEGORY	CHECKS	NC	DESCRIPTION OF THE NON-CONFORMITY
9.1.1	Policy of checkof the accesses	Aaccess control policy must be defined, documented and updatedbased on the requirements of business and information security	□	
9.1.2	Access to networksand services of network	Users mustonly be provided access to networks and network services for whichuse were specifically authorized	□	
9.2.1	Registration and it's-registration of users	A formal process must be in place of registrationand de-registration for enable the assignment of rights to access	□	
9.2.2	Provisioning accesses of users	A formal process must be in place forthe assignment or revocation of rights fromaccess for all types of users and for all systems and services	□	
9.2.3	Management of rights of access privileged	The assignmentand the use of access rights privileged mustbe limited e control yourself	□	
9.2.4	Managementfrom the information secret of authentication	The assignment of informationsecret of authenticationmust be checked through a management process formal	□	
9.2.5	Review of rights of access of users	Asset managers must reviewrights at regular intervals fromuser access	□	
9.2.6	Removalor adaptation of the rights of access	Access rights of all staff e of users of external parties a informationand processing facilities information must be removed upon termination of the employment relationship, delcontract or agreement, oradapted to each variation.	□	
9.3.1	Use of information secret of authentication	Users mustbe required to follow the organization's practicesin the use of informationsecrets of authentication	□	

15	RELATION WITH SUPPLIERS			
POINT	CATEGORY	CHECKS	NC	DESCRIPTION OF THE NON-CONFORMITY
15.1.1	Policy for the security of information in relationships withproviders	The security requirements of the information formitigate risks associated with access to assets of the organization by providersmust be agreed with the suppliers themselves and documented	□	
15.1.2	Address the safety inside of of the agreements withproviders	All safety requirements information must be establishedand agreed with each supplier who might have access, elaborate, archive, transmitor provide infrastructure components IT for information of the organization	□	
15.1.3	Supply chain of supply for ICT (Information and communication technology)	The agreementswith suppliers must to includethe requirements to address i security risksfrom the associated informationto services and to productsof the supply chain for ICT	□	
15.2.1	Monitoring and review of services of providers	Organizations must regularly monitor, reviewand submit to audits the provision of services by of suppliers	□	
15.2.2	Management of changes to the services of providers	Changes to the provision of services by the suppliers, including the maintenanceand the improvement of current policies, procedures and controls for theinformation security, mustbe managed, taking into account the criticality of the information business, systemsand processes involved and the reassessment of risks	□	

16	SAFETY INCIDENT MANAGEMENTOF INFORMATION			
POINT	CATEGORY	CHECKS	NC	DESCRIPTION OF THE NON-CONFORMITY
16.1.1	ResponsibilityAnd procedures	They must beestablished responsibilities and procedures of management to ensure a quick answer, effective and orderly to the accidents related to the security of information	□	
16.1.2	Report of the events concerning at the safetyfrom	Events related to the security of information must be reported as much quickly as possible through appropriate channels management	□	
16.1.3	Report of the points of weakness concerning at the safetyfrom the	It must be requestedto all staff and to the collaborators who use the systems informative and the services of the organization of to recordand report each point of weaknessrelating to the security of information that has been observed or suspected in systems or services	□	
16.1.4	AssessmentAnd decision on events concerning to safety from the	Security related events must be evaluated and it must be decided if classify them such as incidents related to safetyinformation	□	
16.1.5	Response to accidents concerning to safety from the information	Yes must respond to incidents related to safetyof the information in accordance with documented procedures	□	
16.1.6	Learning from accidents concerning at the safetyfrom the	Acquired knowledgefrom the analysis and from the solution of accidents related to safetyinformation must be used to reduce likelihoodor the impactof future accidents	□	
16.1.7	Collection of evidence	The organizationmust define and apply appropriate procedures for identification, the collection, acquisition and retention information that may be used as evidence	□	