0.7 Requirements of the standard and application by the organization

In the following paragraphs, the organization has done soto illustrate, in a synthetic and schematic way, the way in which it fulfills the requirements of ISO 27001: 2017. Each paragraph is dedicated to a specific point of the Standard so as to provide all interested parties with a clear picture of the functioning of the information security management system.

STRUCTURE OF THESTANDARD AND MANUAL SECTIONS	
1	Scopeand field of application
2	Normative requirements
3	Termsand definitions
4	Context
5	Leadership
6	Planning
7	Support
8	Operating activities
9	Performance
10	Improvement

The contents of the manual give priority to summary information. Each point, however, refers the in-depth analysis to other documents such as procedures and forms of the same system. Any misunderstandings or need for clarification can be reported to the information management system manager who is:

Doctor Tomas KG Clinton

CONTEXT OF THE ORGANIZATION

MAN-04

Understanding the needsand the expectations of interested parties

Monitor the contextit also means continuously identifying the parties concerned with the protection of information and their specific needs for confidentiality, integrity and availability of data. Thanks to the PROC-400 - Context monitoring procedure, the organization always keeps the needs of those interested in protecting information under control, thus being able to provide them with the right guarantees regarding the controls used to protect information.

The organization, thanks to the application of the PROC-400 procedure- **Context monitoring**, exercises an importantobservation activities of the internal and external world, creating moments of formal information sharing during which the participating subjects identify and re-examine influential factors, interested parties and the needs of the interested parties.

Scope of the management system

In this section of the manual, the organization has established the scope of the information security management system.

Object of information security:

- Data concerning the identity, functioning and structure of the subject or of the clients and suppliers
- Data regarding the way in which the organization carries out statistical analysis activities eg: data mining

Treatment processesinformation: "Primary" processes (or alternatively also called operational processes)

The organizationcarries out its consultancy activity for data mining through operational processes ranging from the initial collection of the client's data to the supply - to these - of the results of the analyzes. These processes that fall within the scope of this management system are the following and are reported, with their original name, by the corresponding procedures drawn up, applied and stored in the organization:

- Requirements
- Design
- Outsourcing
- Production
- Preservation
- Non-compliant output control

5 Leadership

Politics

ThereInformation Security Policy has been defined by the organization's Leadership, in such a way:

- To be appropriate for the purposes of the organization
- To constitute a reference framework for setting safety objectives
- This includes a commitment to comply with applicable and information security requirements
- The commitment to continuous improvement of the management system must be maintained

The Security Policyinformation is made available as documented information, is communicated within the organization, is made available to interested parties.

It's still:

- Therepolicy is accessible on the organization's institutional website
- It is communicatedto company staff by sending them via e-mail
- It is posted on the notice boards of the organization so that it can be visible to staff and any visitors

The organization adopts twolevels of information security policy:

- The highest level, level A, documents the general policy within MOD-520 - Security Policy **information**.
- The lower level, level B, documents topic-specific policies. The specific policies are reported in the procedures in reference to each control of Annex A for which they are envisaged. They are:
  - Policy forthe use of portable devices
  - Telework Policy
  - Control policyof access
  - Policy on the use of cryptographic controls
  - Screen policyand desk clean
  - Backup policy
  - Transfer Policyinformation
  - Policy for itsafe development
  - Policy for thesecurity in relations with suppliers

The term policy used in the meaning of the standard, translated into Italian, means "rule" or "rules". The organization, however, understood the term policy in a broader sense, developing real policies in a general sense with respect to the subject, reserving to the procedures the task of explaining the individual "rules" that govern the functioning of the security processes .

6 Planning

Planning

In relation to the risks and their extent, the organization has drawn up the Information Security Plan contained in the MOD-610-B-Information Security Plan form with which it has activated the information security controls. The plan is one of the key documents of the management system as it explains how the organization intends to protect information and reassures third parties about how the organization applies security controls to the information it processes and processes.

Security controls in management procedures

The security controls activated by the organization are those indicated in Annex A of the ISO 27001: 2017 standard (this is an annex to the standard in which there is a list of measures to be taken in correspondence with certain circumstances such as physical protection facilities, network access control, information backup, etc.).

These controls have been integrated into the management procedures, that is, those procedures that govern the entire operation of the company through its "primary" processes also defined as "operational" such as: design, production, etc. and support processes such as context analysis, planning, management review, etc.).

The integrationwas performed as follows in the example. The text is taken from the management procedure PROC-710

- **Asset management**,in which, the security controls of Annex A, with their number, have been integrated into the management activities.

[control 8.1.4] Return of assets

All the staffand external party users must return all organization assets in their possession at the end of the period of use,of the contract or agreement entered into.

The organization's employment contracts expressly provide for the return of all the assets of the organization in their possession at the end of the period of employment, the contract or of the agreementstipulated.

Therereturn is recorded in the module MOD-710-M- Asset inventory. The registration the successful return consists in the assignment, on a specific date, to another manager or to the organizationitself (RGSI) that holds it in charge pending a new assignment.

[control 8.3.1] Managementremovable media

Procedures need to be developedfor the treatment of removable media according to the classification scheme adopted from the organization

The organization, within the moduleMOD-710-M- Asset Inventory has identified a field with which determine if the assetit is removable. This "removable", commonly associated only with memory devices (eg: USB sticks, portable hard disk, etc.), is extended to all physical assets that can be transported (maybe draggedor stolen) outside the organization

6 Planning

Controls in safety procedures

For some controls present in Annex A of the standard it was necessary to draw up separate procedures, which unlike the others (management procedures) are configured as "safety procedures". In fact, they do not regulate the functioning of the organization but regulate the implementation of information security controls.

These procedures that bear the prefix PSI (information security procedure) report, next to the acronym also the number of the control with which it is identified in Annex A of the standard. They are:

- PSI-06- Teleworking and information security
- PSI-09- Access control
- PSI-10- Encryption
- PSI-11- Physical and environmental security of information
- PSI-12- Operational safety
- PSI-13- Communications security
- PSI-14- Acquisition, development and maintenance of systems
- PSI-16- Management of information security incidents
- PSI-17- Operational continuity management of information security
- PSI-18- Compliance

The objectivesof the organization

There The strategic purpose of the organization, with reference to the management system in question, is the protection of information from the risk of loss of confidentiality, integrity and availability.

The organization, with the intent to focus efforts on the pursuit ofthis purpose towards specific and measurable goals, has established safety objectives, measured through the safety index, with reference to:

- Human resources security
- Network securityand communications
- Safetyin the quality of training
- Software security
- Security in computing devices
- Safetyof the headquarters and archives
- Safetysystems and safety devices

When we refer to "human resources security" we are not referring tosecurity of individuals but to the security of information with respect to the risks that could come from people.

People and skills

Given the influence that human resources can exert on information security, the organization has drawn up a procedure that integrates the security controls reserved for personnel (from Annex A) through a series of steps for which it must:

- Determine the skillsnecessary for human resources who perform work activities under the control of the organization and which influence the performance and effectiveness of the ISMS
- Establish reliability requirementsof people who have to handle sensitive information
- Ensure that human resourcesare reliable and competent based on appropriate education, training, or experience
- Undertake actions to acquire the reliability and the necessary skills and evaluate the effectiveness of the actions taken
- Retain appropriate documented information such asevidence of reliability and skills

The procedureestablishes that, following the recognition that allows us to understand which figures it needs, a careful selection of candidates is carried out who possess specific requirements relating to:

- Educational qualification
- Experiences
- Previous knowledge
- Competence
- Awareness

The hiring of staff, in this procedure,it is a delicate phase in which security controls are applied relating to contractual aspects for which specific commitments are made relating to the confidentiality and use of the assets made available by the organization.

Personnel, in relation to their role, are constantly trained and made sensitive to information security risks. The management applications related to the PROC-720 - People and skills procedure allow you to keep under control the training activities and the quality of the training carried out. The organization, in fact, is aware that the training and awareness of human resources are the main measures for the prevention of risks.

Even though the management system is perfectly conceived with everyoneits controls, it could be rendered useless by the behavior of people who knowingly circumvent the established rules in order to cause damage. In this regard, the procedure establishes the functioning of the disciplinary process to which personnel who break the rules could be subjected.

OPERATING ACTIVITIES

MAN-08

Point 8 of the ISO 27001: 2017 standard was managed by the organization with the aim of tracing the operational processes in all their phases to keep under control the risks that are present in all those activities that relate the organization to the customer in order to provide them with the product / service that they have requested from the organization.

The organization in thehis business actually sells data analysis services. The operational processes (also defined as primary) are those that start from the collection of the requirements that the customer determines for the request for their service product up to the actual production of the service product and its control during the release phase.

To facilitate alignment with other present and future management systems in the organization, point 8 of the standard was developed by simulating (in the sole definition of the process name) a sort of parallelism between the requirements of ISO 9001 relating to management for quality and operational processes of the organization.

The governing proceduresin fact, these processes have been assigned names that recall the sequence of operational activities presented by ISO 9001.

The opportunity tothis parallelism which, as can be seen from the actual application of the documents to the system, will simplify the understanding of the entire production process, is made possible by the fact that ISO 27001 and ISO 9001 have the same structure (High Level Structure) conceived by the institutions of standardization precisely to facilitate communication between different and coexisting management systems.

The (primary) operational processes governed by the corresponding procedures are as follows:

- PROC-812- Requirements
- PROC-813- Design
- PROC-814- Outsourcing
- PROC-815- Production
- PROC-816- Preservation
- PROC-817- Control of non-conforming outputs

Within each procedurethe controls reported in Annex A of ISO 27001: 2017 have been integrated.

PERFORMANCE EVALUATION

MAN-09

Performance evaluation

Audits

The organization has prepared the procedure with which it carries out audits relating to compliance:

- Of the management system to the requirements of the ISO 27001: 2017 standard
- Control procedures established by annex A of the standard
- Of the behavior of people to the prescriptions contained in the procedures

The procedure PROC-920 - Internal Audits governs all phases of auditing activities such as:

- Planning
- Preparation
- Execution
- Registration
- Closure
- Archiving
- Audit monitoring

Also the audit processit is kept under control from a statistical point of view by management applications. In this case the process is monitored, in its safety index, through the MOD-920-E - Monitoring auditing module in Excel which automatically detects the level of safety in relation to the way in which the organization manages non-conformities and prevents them. the repetition.

Themanagement review

The organization, to ensure that the management of the management system is always oriented towards the strategic objective and does not suffer from drift towards moments or situations of deadlock, inactivity or inefficiency, it organizes periodic review activities.

At the meetings ofmanagement review, as established by the procedure governing its functioning PROC- 930 - Management review, top management, process managers (RDP) participate according to their respective skills and the personnel employed in information security.

10 Improvement

The organization providesto remove and prevent any obstacles that may prevent the protection of information or compromise its security. To this end, when it detects a non-compliance that is manifested through intentional behavior or behavior attributable to distraction, it proceeds with a thorough examination of the non-compliance.

There procedure PROC-1010 - Non-conformities and corrective actions focuses attention on the analysis of the causes of the Notcompliance and determines the criteria for developing corrective actions that can:

- Remove unwanted effectsof non-compliance
- Prevent thatsuch non-compliance occurs in the same context or in other circumstances

TheThe steps illustrated in the procedure are as follows:

- Classificationof non-compliance
- Detectionof non-compliance
- Registrationand analysis of non-compliance
- Determination of corrective action
- Implementation of the actioncorrective and verification

PROC-1020- Continuous improvement

For this point of the standard, the organization has drawn up the procedure dedicated to the continuous improvement of the safety and efficiency performance and effectiveness of the management system, even in a broader sense. In this sense, the organization has set up a sort of "research & development" office which it has identified in an improvement group consisting of some RDPs (process managers) and other personnel dedicated to information security.

Likeexplains the procedure in detail, the Improvement Group is entrusted with the "mission" of analyzing the results of the information security management system and developing an improvement strategy.

Thereimprovement strategy contained in module MOD-1020-A Improvement strategy is presented by the improvement group by senior management at the management review. The presentation takes place in an official manner and, depending on the opportunities, takes place in the presence of the organisation's financing members and in the presence of all interested parties.

Therestrategy will be made operational and implemented under the guidance of top management by all those involved and indicated in the relative documentation.