ISP N° 0443 E

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC

Signatory of EA, IAF and ILAC Mutual Recognition Agreements

GERICO SECURITY SRL

INSPECTION BODY

INSPECTION ACTIVITY REGULATION ACCORDING TO ISO/IEC 17020

Document prepared by:	Giustino Fumagalli
Document verified by:	CDA
Date:	04 January 2023
Version:	2.0

Version	Date	Explanatory notes
1.0	01/02/2020	First issue
1.1	13/03/2021	Update following the findings of Accredia on 04/03/2021
1.2	01/08/2021	Update in accordance with DPCM 81 of 14 April 2021 published on 11/06/2021
1.3	29/12/2021	Revisions following the visits of Accredia & Accreditation
1.4	29/10/2022	Revisions following the audit of Accredia
2.0	04/01/2023	Introduction of Vulnerability Scan

Table of contents

1 GENERAL PROVISIONS

1.1 Preface

Gerico Security Srl having its registered office at 2 Passerini Street, Monza (MB), carries out inspections compliant with ISO/IEC17020 through its "Inspection Body"[1] (IB). Such activities regard information security and cybersecurity of any private or public company type.
The term Inspection means "the examination of a process, service, design assessing its compliance with specific requirements or general requirements according to professional judgment[2].

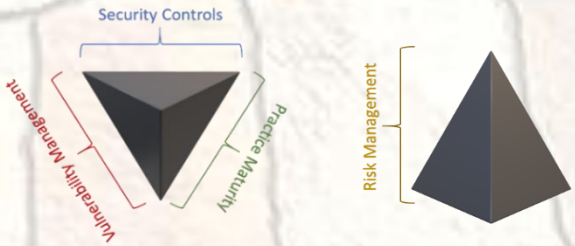
1.2 Purpose and Scope

The purpose of this regulation is to determine the conditions and methods of the Inspection Body (IB or OdI) activities of Gerico Security Srl as follows:

Scheme	Category	Field	Subfield	Range	Stage	Requirements
ISP	Process / Service	Information and Communications Technology	//	Inspection and verification of information security and cyber security	• Pre-service phase · In-service phase	National Cyber Security Framework – CSF 2.0 February 2019
ISP	Process/ Service	Information and Communications Technology	//	Inspection and verification of information security and cybersecurity	• Pre-service phase • In-service phase	Cyber Security Framework National – CSF 2.0 February 2019

All processes related to the inspections, the inspector's management activity and maintenance of the Inspection Archive are considered within the scope.

An organization is inspected to photograph the existing situation at a given moment according to the four dimensions of the Cyber Security Pyramid: three at the base of the Pyramid and one at its height as shown in the figures below:



[1] According to ISO/IEC 17020:2012, Gerico Security Srl carries out the inspection activities as a type C Inspection Body (clause 4.1.6 (c) of.ISO/IEC17020).
[2] Contextualization of the definition of Inspection sets forth in ISO 17000:2020 (6.3) : *examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements.*

The inspection is carried out according to specific criteria as follows:

- Objectivity, measuring the state of art according to given parameters,
- Neutrality towards partisan beliefs,
- Impartiality and absence of conflicts of interest.

The results are provided with measurable and comparable metrics considering the maximum objectives achievable by the inspected company. Thus, the organization and third interested parties can use the inspection results to assess the Cyber security maturity according to objective criteria guaranteed by a reliable Third-party Body.

1.3 Inspection Archive

All inspection documents are digitally signed and kept in a dedicated “Inspection Archive” for a minimum period of 5 years. Only IB’s authorized personnel are allowed to access the *Archive*. All documents are stored in the *Archive* as “Confidential” in compliance with the information classification of Gerico Security Srl.
The Inspection Archive enables the IB to provide evidence concerning the inspections and manage possible requests for Attestation of the Reports from interested third parties that had lawfully received such reports. No document or evidence of the inspected company is retained by the Inspection Body and/or its Inspectors.

1.4 Request for attestation of the Inspection Report

The Cybersecurity state of an organization is attested in the Inspection Report and shown in a Inspection Certificate. It is mainly used by the Inspected company to demonstrate its Cybersecurity maturity to third parties (clients, partners, Regulatory Bodies, Public Administration).

The Inspection Body attests the authenticity and truthfulness of the Inspection Certificate by digitally signing all documents of the Inspection.
It is possible to make requests for attestations of authenticity and truthfulness by sending reasoned requests with a copy of the Report in your possession at: OdI@gerico-sec.it

When the IB receives the request for attestation from a third party, the Technical Responsible Officer verifies the grounds of the request and the authenticity of the Inspection Certificate copy by comparing the digital signatures of the documents.

The IB responds within 10 working days of the date of receipt confirming the attestation or denying the authenticity of the copy received.

2 LAW AND RULES OF REFERENCE

The present document is based on the law and rules as follows:

- ISO/IEC 17020:2012 “Conformity Assessment – Requirements for the operation of various types of bodies performing inspections”,
- ISO17000:2020 “Conformity Assessment – Vocabulary and General principles”,
- ILAC P15:05/2020 “Application of ISO/IEC 17020:2012 for Accreditation of Inspection Bodies”,
- Accredia - RG-01 – Regulation for the accreditation of Certification, Inspection, Verification and Validation Bodies- General Part,
- Accredia - RG-01-04 – Regulation for the accreditation of Inspection Bodies,
- Accredia - RG-09 – Regulation for the use of the Accredia Mark,
- ISO/IEC 19011:2018 “Guidelines for auditing management systems”,
- ISO 31000:2018 “Risk management” – Principles and guidelines”,
- D.lgs. 231/2001 – provides for direct administrative liability of legal entities, companies and associations,
- The (UE) 2016/679 Regulation on the protection of natural persons regarding the processing of personal data and on the free movement of such data,
- D.lgs. 101/2018 providing for the alignment of the Italian privacy policy (D.lgs. 196/2003) to the UE Regulation
- D.lgs. 81/2008 – On the protection of safety and health of workers. Health and safety in the workplace.
- UNI 10459:2017 provides for Professional activities – Professionals operating in the field of security – Knowledge, skills and competence requirements,
- NIST CSF 1.1 16 April 2018,
- Cini - " National Cybersecurity and Data Protection Framework " – 2019 - V2.0,
- ISACA - "IS Audit/ Cybersecurity Assurance: based on the NIST Cybersecurity Framework Audit Program" – 2016,
- D.Lgs.65 18/05/2018 “Transposition of the (UE) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union”.
- DPCM 81 of 14/04/2021 “Regulation concerning notifications of incidents impacting networks, information systems and IT services (art. 1, paragraph 2, let. b), of the Decree-Law n. 105 of 21 September 2019, converted into law no. 133 of 18 November 2019 and providing measures to guarantee high security levels.” Published in the O.G.U. on 11/06/2021.
- DL.105 of 21/09/2019 “Urgent measures on the cybernetic national security perimeter” converted into law n.133 18/11/2019 on 20/09/20219,
- IAF MD 4:2018 – IAF Mandatory Document for the use of Information and Communication Technology (ICT) For Auditing/assessment Purposes Issue 2.

3 DEFINITIONS AND ACRONYMS

- **ACCREDIA**: is the sole accreditation Body in Italy appointed by the Italian government attesting the competence, independence and impartiality of the inspection and verification bodies and laboratories, the status of conformity of the goods and services. According to the UE Regulation EC 765/2008 and the international standard ISO/IEC 17011, every member state has its national accreditation body. ACCREDIA operates in Europe as a member of EA (European cooperation for Accreditation) and works internationally as a member of IAF (International Accreditation Forum). Operating as an impartial authority, the accreditation Body guarantees the reliability of the activities carried out by the bodies and laboratories. It provides a socially important activity working for the public good. Accredia is an impartial and independent Body which ensures that the accredited bodies and laboratories fulfil the requirements of the specific standards. It guarantees the objectivity and authenticity of the attestations issued in the market, safeguards the health of consumers and environmental protection.
- **Accreditation:** it attests the degree of quality of the (certification and inspection) activity of an accredited Body, attests the conformity of management systems and skills with the requirements of the law and international standards. Accreditation is a safeguard giving confidence of:
    - Impartiality: all interested Parties are represented within the Body.
    - Independence: the auditors and committees responsible for issuing the certification/ report guarantee the absence of conflicts of interest between the body and the organization seeking certification.
    - Fairness: European standards prohibit the provision of advice either directly or through related companies.
    - Competence: accreditation mainly certifies that the personnel involved in the verification activity are culturally, technically and professionally qualified.
- **BoD** – Board of Directors of Gerico Security Srl.
- **Client –** the company for which the inspection activity is carried out. It may coincide with the inspected company or be an interested third party in which case the inspection is agreed upon and authorized by the company.
- **Cybersecurity –** it generally refers to information technology designed to protect information systems against access or attack. This document provides a more extensive definition of the processes and technologies for the security of information managed, created, stored and shared on interconnected devices through a local and/or public geographic and/or private network ensuring confidentiality, availability and integrity of data.
- **Board – The Board of** Gerico Security Srl is the Board of Directors of the company.

- **ToI – Team of Inspection**, a team of qualified guided Inspectors who carry out an Inspection.
- **Qualified Inspectors –** Inspectors qualified by the IB and therefore authorized to carry out inspection activities on behalf of the IB. Such professional qualification is a formal process of the IB which formally verifies skills, competence, knowledge and ethical values of the inspectors.
- **Inspection[3] –** conformity of assessment of a process, service, product, design with specific requirements or, on the basis of professional judgement, with general requirements.
- **Organization** – Legal entity or company subject to a formal Inspection.
- **IB – Inspection Body (OdI –"Organismo di Ispezione"), it is a separate division of** Gerico Security Srl, structured and organized to conduct formal and unbiased information security and cybersecurity Inspections of an organization.
- **Information Security –** protection of Confidentiality, Integrity and Availability of information regardless of whether it is kept in electronic, physical or paper-based format throughout the phases of its life cycle from its creation to its controlled destruction: its processing, storing and archiving, transmission and/or dissemination to third parties by using digital devices, physical tools or orally communicated.
- **Verification –** Activity carried out in compliance with the DPCM 81 of 14 April 2021 (Art.8 paragraph 6) D.L. n.105 of 21 September 2019 "Urgent measures on the cybernetic national security perimeter" converted into law n.133 18/11/2019 (Art.1, paragraph 6 letter c) on 20/09/20219
- **Vulnerability Scan,** process performed by using automatic tool of identifying security weaknesses and flaws in systems and software.

[3] Contextualization of the definition of Inspection in ISO 17000:2020 (6.3) : *examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements.*

4 ISPECTION BODY GENERAL REQUIREMENTS

4.1 Inspection body responsibility

The Inspection Body (IB or OdI – “Organismo di Ispezione”) has the overall responsibility for conducting the inspection process based on the criteria of impartiality and completeness. Therefore, it:

- adopts a model to ensure a formal process for conducting information security and cyber inspections which can be evaluated as reliable and recognized by third parties,
- ensures the complete execution of the Inspection activity within the perimeter as defined in the contract with the Client,
- evaluates the appropriate times and methods of the Inspection to fulfil the activity,
- guarantees the competence, professionalism, and ethical values of the IB inspectors and personnel,
- protects the interests and confidentiality of the inspected company’s processes, information, knowledge, strategies and all information learned during the course of the Inspection,
- meets the needs of the Inspected Company minimizing effort and burdens on business to the smallest possible degree to conduct the Inspection
- protects the inspected Company against damage and increased risks
- adopts custody process of the documents and data of the Inspection results to be retained over time and within a defined period to demonstrate the Inspection activity and its results

The activity of the Inspection Body of Gerico Security Srl provides a photograph of the state of security at a given moment in time. Therefore, the Inspection Body is not responsible for possible noncompliance or shortcomings which might be detected through continuous and systematic on-site inspections.

4.2 Impartiality and Independence

Gerico Security Srl has defined and documented its structure, organization and organizational measures in compliance with its Ethical Code to conduct unbiased inspections of Information Security and Cybersecurity. In this respect, an “Inspection Body” (IB), formally independent and whose management is committed to the safeguard of impartiality, has been set up.

Possible conflicts of interest are considered and handled to safeguard impartiality of its work. The conflicts of interest can be those arising from and within the Inspection Body, for example as regards the personnel appointed or those arising from the activities of other people, bodies, companies. In particular, the IB provides a proactive process to prevent the potential conflicts of interests arising from new professional assignments of the Body and the personnel of inspection.

The Inspection Body carries out an unbiased activity with respect to its clients without being affected by influences which might have impacts on the results of the Inspection. Therefore, the inspections are carried out in accordance with a methodology nationally and internationally recognised so as to safeguard impartiality, completeness and objectivity of the inspection.

4.3 Confidentiality

Confidentiality of Client Information is a founding principle of Gerico Security Srl since it considers as confidential all the activities carried out with reference to the objects and topics covered, the nature of the activity and information processed. Therefore, Gerico Security Srl ensures that any information, directly or indirectly learned in the course of the activity conducted on behalf of the client, is not disclosed for the purpose other than the Inspection or used for undue business financial benefits.

Gerico Security Srl is ISO/IEC 27001:2013 certified and has adopted an Information Security Management System. Its principles and security measures also apply to the Inspection Body. In this regard, Gerico highlights the importance of its Information Security Policy available on its institutional website. It is understood as a set of objectives and strategic planning for managing and protecting the information stored and treated by the Company, for the key resources and IT processes for information processing.

The Information Security Policy defines:

- The security objectives,
- The conformity requirements with law, standards, and sectoral best practices,
- A logical organizational and management model for securing information,
- The requirements for the fulfilment of information security objectives.

The objectives of the security Policy refer to the need to reduce the risks to confidentiality, integrity and availability of information of the company and clients to acceptable limits.

According to the risk level determination, as defined by Gerico Security's Board, the risks exceeding the acceptable levels are reduced to acceptable limits by implementing countermeasures which cannot be violated unless it is done intentionally. Such countermeasures are defined in the analysis methodology and information risk management adopted by Gerico Security. They apply to different levels of protection, thus should a countermeasure fail, it can be replaced with another different safeguarding measures for an appropriate and balanced protection system ("defence in depth").

In particular:

- Confidentiality is protected through appropriate countermeasures to prevent unauthorized access to information or uncontrolled dissemination,
- Integrity is protected through appropriate countermeasures to prevent unauthorized modification of information or damage to its physical format or semantic content,
- Availability is protected through appropriate countermeasures to consent the access of authorized personnel to the resources needed to fulfil their activities.

Intervention measures are intended as a continuous process of risk detection, analysis, assessment and the choice of the best preventive and management strategies for the governance of Gerico Security Srl's Security Information.

Finally, the personnel and the qualified Inspectors, or those about to be qualified, are made aware and contractually bound to information confidentiality, integrity, and availability regarding clients, inspections and the IB.

4.5 Management System Policy of the Inspection Body

The Board of Gerico Security Srl has decided to provide the Inspection Body with an Inspection Management System. The B. has established, documented, and maintains the inspection Body policy and its goals according to the ISO 17020:2012 purposes. It promotes and ensures the policy awareness of all the Inspection Body's executives and staff. In particular:

The Board of Gerico Security Srl acknowledges the importance of providing its services in adherence to the legal requirements and according to the clients' needs. It promotes the accomplishment of an Inspection Management System and undertakes a continuous improvement approach to its effectiveness through a periodical identification of quantified and verifiable objectives, aimed at satisfying the Client and ensuring unbiased and quality inspection activities.

To this end, the Board defines the policy and the following objectives:

- *enhance the positive image of a reliable and competent company establishing trust with clients,*
- *meet legal requirements, regulations, and contractual obligations,*
- *ensure the needed training and information among personnel and staff,*
- *verify if the services provided meet the requirements of the sector and clients and measure the client' satisfaction,*
- *guarantee the impartiality of the Inspection Body,*
- *keep confidentiality of the information handled and processed in the course of the inspection,*
- *observe ethical standards during security inspections,*
- *ensure a continuous improvement of the Management System activities reducing risks.*

The Board undertakes to spread the Inspection Body policy among all parties disseminating its information as documented information. In addition, the Management undertakes to periodically review all activities, processes and results to achieve the desired level of improvement.

The Board undertakes to maintain the independence of the Inspection Board and unbiased judgement towards the inspected companies.

The Boards appoints a Responsible person for the Management System who works to ensure the MS effectiveness over time.

4.6 Inspection methods and procedures

The Inspection Body has defined a formal methodology to ensure:

- Completeness of the evaluation activity
- Uniformity of judgement
- Fairness of judgement

The methodology is based on the best practices of the sector in accordance with the criteria of completeness and rigor ensuring impartiality within Security Information and cybersecurity to provide unbiased judgement, independent from the influence of third-party within its conformity decisions.

The evaluation of security aspects is assessed in accordance with objective criteria comparable over time in order to ensure uniformity ed fairness of judgement.
The inspection results enable the:

- Overall evaluation of the inspected company maturity and capability to ensure Information and Cyber Security
- Objective measurement of the security state at a given time
- Comparability of the company's security maturity levels over time and with respect to other companies.

The inspection methodology is structured and formalised. Possible changes to the methodology are based upon rigorous criteria of necessity and opportunity such as the evolution of legal and standard requirements.
The methodology changes are verified to detect deviation results in comparison with the previous version then, the correction measures needed are studied. The impossibility of avoiding deviation results is formally communicated to the client seeking the attestation indicating the differences of judgement within the different methodology versions.

The Inspection Body regulates the entire process by setting forth the operating procedures. The technical Responsible manager of the IB and the inspectors are required to abide by inspection procedures while performing their tasks and related activities.
The initial phase of the process provides an evaluation of impartiality and formalization of the contractual activity then, the inspection activities are carried out and finally, the process is concluded, and the inspection documentation is stored. The inspections are conducted in accordance with standard methods following a schedule agreed with the inspected company
The inspection is led by one or more Inspectors under the final responsibility of the Technical Responsible manager of the IB that signs the results.

4.7 Qualified Inspectors

Only the Inspectors who are Qualified by the IB are allowed to conduct inspections in accordance with the formal procedures; they are required to:

- ensure adherence to law, regulations, administrative measures, and general provisions, to refrain from illicit actions violating the principles of moral rectitude, honour, and dignity,
- adopt flawless behaviour, act in good faith to collect only the information they need to carry out their tasks, refrain from using it for personal gain or for purpose of damaging the inspected company,
- respect the inspected company, its personnel, mission, and all interested parties,
- be diligent and conduct quality inspections following the quality inspection standards and fulfil the commitments undertaken,
- respect confidentiality: collect only information that is necessary for the task and once learned cannot be disclosed and used solely in connection with the inspected organization's benefit,
- adopt unbiased judgement: evaluations are carried out and decisions are made without being influenced by the inspected organization, its business sector, country of origin, company's policy, management style, composition of personnel in terms of age, gender, ethnicity, political and religious beliefs,
- adopt uniformity of judgement in the presence of identical or similar situations within the company or among different organizations.

The Inspected Organization may request a substitution of an Inspector before the commencement of the Inspection and within 1 working week upon receipt of the appointment of the inspector by sending a well-founded request. If the Inspection activity is formalized near the activity start date, the inspected company will automatically agree to waive any objections relating thereto.

4.8 Evidence management

The inspectors ensure the utmost diligence in managing inspection evidence. They access only the evidence that is needed for the purpose of the task.
The inspectors guarantee to keep confidential the inspected company's evidence and information.
As far as possible, evidence is kept within the perimeter of the Inspected Company, where it is kept in a digital format, it can be accessed in read-only mode without saving a copy locally.
Evidence is returned to the Inspected Company or disposed of.

4.9 Records of the Inspections

All information collected by the inspectors throughout the activities is recorded in a dedicated inspection Checklist. The Checklist is signed by the Technical Responsible Officer of the IB and stored for securing evidence in case of appeals or other needs. it is kept in the Inspection Archive together with the other information of the Inspection activity.

4.10 Control activities of the Accreditations Bodies

As an ISO/IEC17020 accredited Inspection Body, Gerico Security Srl is subject to Accreditation Bodies[4] audits. Accreditation bodies are in turn audited by their auditors who carry out inspections at the headquarters of the Inspection Body and perform the inspections together with the IB Inspectors to ensure adequacy, the procedure conformity and verify the inspectors' behaviour. Therefore, the purpose of the Accreditation Body presence is to verify the appropriateness and the conformity of the Inspection Body with reference to its judgement uniformity.
ACCREDIA is responsible for its appointees and their accompanying activities. The Inspected Company may require a commitment of confidentiality from Accredia.
If the Inspected Company denies its appointees' access to the inspections without reasonable grounds, the Inspection activity in progress can be blocked.

In addition, ACCREDIA can independently verify the information handled by the Inspection Body of Gerico Security Srl, for example by contacting its Inspectors or the Inspected Company during or after the Inspection.

[4] ACCREDIA in the Accreditation Body in Italy.

5 RESPONSIBILITY OF THE CLIENT

5.1 Responsibility of the Inspected Company

The Inspected Company is required to permit and ensure the orderly and complete execution of the Team of Inspection (ToI)'s activity by:

- agreeing on a final Inspection Plan with the Inspection Body and defining places, processes, technologies and references in the perimeter of the Inspection,
- ensuring effective cooperation with the IB, appointing an internal contact person for addressing any issue which may arise before and during the Inspection,
- refraining from actions which may be an obstacle to the Inspectors' activities,
- ensuring access to the area subject to Inspection in accordance with the Inspection Plan,
- supporting the IB to access the Systems and technologies to be inspected,
- ensuring access to documents, systems and information according to the IB's requests
- ensuring appropriate times and places needed to interview the contact people selected,
- accepting that all documents of the Inspection are kept by the IB.
- accepting the possible attendance of ACCREDIA's inspectors as observers.
- Answering ACCCREDIA's questions regarding the Inspection methods used by Gerico Security Srl's Inspection Body.

If the Inspected Company is not the Client seeking the Inspection, the Company has to:

- Agree on inspection activities, times and perimeter,
- formally authorize the IB to carry out the Inspection and provide the Client with the Inspection Report in a Public Report format.

5.2 Responsibility of the third-party Client

If the Inspection is requested by a different body, company, or organization other than the Company to be inspected, the Client has to:

- Agree with the Company subject to inspection in order to authorize the IB inspection as regards times and the perimeter of the activity,
- Assure the IB that the inspection does not take place against the will of the Company,
- Support the IB and the Company to identify the scope of inspection,
- Accept the results of inspection activity in a Public Report format, avoid asking detailed documents for the Company's exclusive use that are kept by the IB.

6 ISPECTION PROCESS

The Inspection process consists of four subsequent activities described as follows:

6.1 Assessment of impartiality following an Inspection request

Upon request, the Technical Responsible Officer of the IB evaluates the absence of conflicts of interest with respect to previous activities. If they have a conflict of interest, they shall withdraw from the assignment.

6.2 Inspection contract

In accordance with the ISO/IEC 17020 standard, paragraph 4.1.6, the Inspection of security information and cybersecurity can be:

a) conducted on one's own Organization in this case, the Client and the Organization coincide,

b) assigned by a client in order to conduct an Inspection on another Company, "the Inspected Company".

If this is the case: a Client asks the Inspection of another Company, the latter shall grant permission to the IB and agree with it upon the activity on behalf of a third party [5].
Therefore, the Client is required to provide the IB with the authorization form duly endorsed and signed by the Company subject to Inspection **then, the IB can accept and sign the assignment agreement**.

The contract of Inspection is formalized with the Client defining the Inspection scope as follows:

a) Headquarters
b) Processes subject to Inspection
c) Technological context
d) Inspection schedule
e) Methods of Inspection (present parties, video calls, back-office activities)
f) Contact person of the Company and of the Client
g) Permission, authorizations or other conditions needed to the IB
h) Vulnerability Scan in an Information systems perimeter

[5] An Inspection asked by a client other than the Company subject to Inspection can take place, for example, if there are cybersecurity contractual obligations between the parties.

6.3 Inspection Execution

An Inspection is a formal activity which consists of preparatory and closure activities in accordance with the agreement with the Client. The Inspection Body, Gerico Security Srl organizes the Inspection activities in compliance with ISO19011:2018 contextualizing the activities and considering the specific characteristics to be addressed.

The Technical Responsible Officer chooses the Inspectors according to the characteristics of the activity contractually formalized, verifies the absence of conflicts of interest and communicates their names to the Company subject to Inspection. Within 1 working week, the Company may request the replacement of one or more inspectors where reasoned application is made. If the acceptance of the contract is formalized close to the inspection activity, the Inspection Company will waive any objections to the inspector.
The Team of Inspection agrees with the Inspected company on the Places, processes, technologies and support people within the perimeter of Inspection.
Preparatory activities are closed by the Technical Responsible Officer, who analyses the Contract and follows the Client indications providing the IB with an activity compliant with the legal requirements and authorizations needed to inspect the Company.

The inspection is carried out on all the sites, processes and systems in scope by using the “IB Checklist”.

The processes and security measures are evaluated according to the security Practices of the Checklist considering if they apply to the Inspection context (where not applicable, they are eliminated and do not produce effects on the overall evaluation in terms of Score shown in the Inspection Report).

Each security practice of the Checklist is evaluated with respect to the company maturity and consistency according to:

- Security practice Maturity
- Consistency of the security practice implementation

The depth of inspection for each Practice depends on the practice complexity or the method of implementation of the security measure. It is aimed at removing the inspector’s doubts. If the inspector does not have doubts, it proceeds without delay to the next phase without asking for further information from the inspected Company.
The implementation of the security practices is verified by conducting interviews and inspections on the Company’s sites.

Moreover, the applicability of the security practises is evaluated, and the cybersecurity maturity is defined and based on the Checklist results achieving an overall score as shown in Chapter.9.

Vulnerability scanning tests are performed, on external perimeter, with automated tools [6] to assess the management of information system vulnerability in parallel with the evaluation of processes and systems managing vulnerabilities.

6.4 Closure of the Inspection.

After the evaluation of all the security Practices of the Checklist and the Risk Management Security Level, the Team of Inspection provides the Company's contact person with the results in brief highlighting possible criticalities.

The Auditee Company can present additional evidence within 2 working days[7] of the closing meeting to provide explanations with respect to such criticalities.
The inspection report may include further summary notes of the inspection responsible person as regards the Inspection methods, criticalities and/or peculiarity.

After the closing meeting, the Technical Responsible Officer of the IB keeps the report and documentation, verifies consistency and quality, and formally closes the Inspection. The Technical Responsible Officer digitally signs and archives the documentation in the IB Archive as official documents.

[6] Vulnerability Scans are performed, on external perimeter, with the IB's tools in compliance with the Operational Procedure.
[7] Evidence of corrective measures implemented after the inspection visits shall not be taken into consideration.

7 INSPECTION REPORTS AND E DOCUMENTATION

The form of the inspection reports enables the identification and measurement of the status of the Company's security. The Report Certificate is intended to provide:

a) The inspected Company with a clear understanding of the overall security status including strengths and weaknesses,
b) Third interested parties with the security status of the inspected Company without disclosing its confidential information. The inspection results are provided with an Inspection Report. Such Report is associated with an Inspection Certificate, in which:

1) The **Report of Inspection**[8] details the Company's maturity processes as regards its information security and cyber security
2) The **Certificate di Inspection**[9] only indicates the overall organizational maturity levels useful to third parties. If the inspection documentation is updated as a result of appeal, a new edition of the documentation is issued. The prior edition is annulled but not cancelled and kept in the Archive.

The inspection documentation is retained in the "Inspection Archive" for 5 years.

At the end of the Inspection, the digital documentation shared for the purpose of the tasks is securely erased by the IB systems, paper-based documentation is returned to the Company or destroyed upon request.

[8] As regards the Information Security and Cyber activity, the Inspection Report is compliant with ISO/IEC17020:2012 Chap.7.4 paragraph 7.4.3 Report.
[9] As regards the Information Security and Cyber scoring activity, the Inspection Certificate is compliant with the ISO/IEC17020:2012 Chap.7.4 paragraph 7.4.3 Certificate.

8 COMPLAINTS AND APPEALS

The inspected organizations have the right to complaint/appeal in case they disagree with the Inspector's activity and/or its findings.

Whereas the complaints are about ethical or quality conformity of the IB activity and are handled by the Board of Directors, the appeals of the Inspection findings are handled by the Technical Responsible Officer of the IB.

8.1 Complaints

The procedure to file a complaint is set forth and formalised in the Inspection contract between the Inspection Body and the Company subject to inspection.

In particular, the complaints can be sent at reclami@gerico-sec.it supplying all details of the plaintiff, an accurate description of the complaint, and any evidence supporting the complaint. The IB notifies the Company of receipt of the complaint and decides without delay.

The compliant is handled by the Board of Directors which undertakes to answer the plaintiff within 10 working days of the date of receipt.

8.2 Appeals of the Inspection findings

The inspected company has the right to appeal the findings shown in the final documentation of the Inspection (intended as Inspection Report and/or Checklist) within 5 working days of the date of documentation receipt by sending an email with the grounds for appealing at : OdI@gerico-sec.it or via PEC at gericosecurity@pec.it giving the details of the contact person to deal with.

Disagreements and misunderstandings with the inspection evaluations are described by the inspected Company together with the appeal evidence. Evidence cannot concern corrections implemented after the Inspection closure.

The Technical Responsible Officer contacts the contact person of the Inspected Company within 5 working days of the date of the appeal receipt, agrees on an appropriate date for discussion and asks for further evidence regarding the misunderstanding of the Inspection Team.

The Appeal is evaluated by the IB's Technical Responsible Officer, who is the person for managing the inspection activities, as an independent party with the assistance of independent Qualified Inspectors with no conflicts of interest in the Inspected Company.

The evaluation is made in association with the responsible contact person of the Inspected Company. Evidence supporting the appeal is examined. Where the appeal has a reasonable basis, the responsible Manager of the inspection management System will ask the technical Manager of the IB to:

- annul the previous inspection Checklist in the Archive
- annul the previous inspection Report (and the associated Certificate)
- correct the evaluation described in the “inspection Checklist”,
- reissue all the documents of inspection in compliance with the new evaluation, the new version is digitally signed and contains a “Complementary Note” which annuls the previous version.

The IB provides the Inspected Organization with the decision via PEC. Where the inspection documents are corrected, they will be attached therewith.

The appeal is registered in the *Register of Appeals*, indicating timing, motivation and resolution. All evidence digitally provided is securely erased by the IB systems and paper-based evidence is returned to the Company or destroyed upon request.

9 GENERAL PROVISIONS FOR THE INSPECTION SERVICES

9.1 Inspection contract

The Inspection Contract is formalized in a standard format. Modifications or alterations are made solely for the specificity of an Inspection activity, for example where specific mandatory rules must be applied previously or in the course of the inspection. Nevertheless, such modifications need to be compliant with the Ethical Code of Gerico Security Srl without affecting the inspection objectives and principles.

For any modifications to the contract, the party will agree to and sign the changes in writing. Unilateral or conflicting conditions and obligations formalized by the Client will not be valid unless agreed upon in writing.

9.2 Use of the Trademark

The Client or the Inspected Company can use the mark of Gerico Security Srl only with the prior explicit and written consent of Gerico Security Srl. The use of the mark must refer exclusively to the scope and the sites of the Inspection carried out, and to the related Reports and documents issued by Gerico Security Srl. The right to use the Gerico Security Srl mark cannot be transferred to third parties other than the Client or the Inspected Company. Gerico Security Srl uses ACCREDIA Mark according to the general Regulation RG-09 available on the website of ACCREDIA at www.accredia.it. In particular, the ACCREDIA mark is shown in the certificates and reports issued by the Inspection Body within the accreditation purposes. The Client is precluded from using ACCREDIA mark.

9.3 Modification to the Inspection Scheme

The Body of Inspection informs the Client and the Inspected Company of any modifications/amendments to the scheme of the Inspection due to new guidelines of reference and consequent revisions of the Inspection Checklist. It considers the observations received in this regard. The conformity process will consider and manage possible score gaps regarding the previous inspection activities.

The Inspection Body communicates the date of entry into force of the amendments and provides publicity on its institutional website - Gerico Security Srl.

10 INSPECTION METHODOLOGY AND FINAL SCORE

The Body of Inspection of di Gerico Security Srl bases its activity on the international sectoral guidelines of reference as follows:

- "National Cybersecurity and Data Protection Framework ", better known as "National CSF " V2.0 which derives from
- "NIST[10] CSF – Cyber Security framework" V1.1 of the United States Department of Commerce

The CSF provides cybersecurity guidelines for reducing risk to US critical infrastructures and then, also recommended for US companies. Likewise, the Italian CSF was provided as a methodology for meeting the needs of national critical infrastructures according to the Directive (UE) 2016/1148 NIS Directive and then recommended to any national company regardless of their size or sector. Whereas, only National CSF [11] provides further specific data security controls to protect personal data.

The conformity to CSF ensures a complete evaluation of Information & Cyber security aspects according to the *best practices* providing companies with the guidelines on the of Cybersecurity implementation and staying NEUTRAL on the third-party certification aspects. The CSF lists a set of Cybersecurity controls which are divided into Functions, phases in the cycle of an overall security process. Not all controls apply to an organization depending on its size and context. The Inspection Checklist considers possible not-applicable controls accordingly.

The IB has formalized an Inspection Checklist providing automatic scoring methods so as to achieve an objective score as close as possible to the Inspector's evaluation for the purpose of ensuring an equal and uniform process of evaluation.

[10] Cybersecurity Framework | NIST (www.nist.gov/cyberframework)
[11] National Cyber Security and Data Protection Framework (www.cybersecurityframework.it)

10.1 Inspection Results

10.1.1 Score Report provided in a public Report format

The Inspection Report and Certificate provide the final score on the following information security and cybersecurity aspects:

- Adequate security measures and practices
- Maturity level of security practice management
- Management of security vulnerabilities of the systems and applications[12]

These values are provided as percentage “Score” using graphs for a clear understanding.

10.1.2 Score calculation

The number of cyber security controls is based on the maximum number of 117 controls in CSF. On the other hand, the CSF is a valid guideline regardless of the size, type of operating context or inspection scope of a company. According to the guideline, the controls are chosen considering the actual organization. Therefore, some controls may not apply.
Hence, the inspector calculates the score by summing the results of all applicable controls.

Considering that the maximum score depends on the number of the applicable controls, the Inspection Report provides the score as a percentage of the maximum value.

Percentage Score	70,00%

10.2 Score tiers evaluation

The Report and Certificate Inspection scores are displayed in a percentage format**: 100% is to be considered as an ideal value,** realistically difficult to be achieved on the grounds that security information and cybersecurity is a changing process with respect to the growing threats of cyber risks, the new technologies and processes used to defend against such threats and attacks. The table below shows how the scores divided into classes should be considered:

[12] The evaluation of the vulnerability management aspects is completed through Vulnerability Scanning to evaluate the Company’s entire process in place. The Company is not provided with a resolution to the problems identified by the automatic system.

Classes of Score		Evaluation
>=90%	**High**	The organization has a high degree of maturity and control in terms of Information and cyber security. Processes and controls are defined and in line with international best practices, a control system is implemented for maintaining conformity with such practices over time.
>=75%	**Medium**	The organization has a high degree of maturity and control in terms of Information and cyber security. However, there are some weaknesses and aspects of noncompliance with international best practices.
>=50%	**Low**	Information Security and Cybersecurity measures are implemented. However, there is not a well-structured approach, shortcomings and significant noncompliance with international best practices are shown.
<50%	**Very low**	The organization highlights significant Information security and cybersecurity shortcomings.

<end of document>