

# **TISAX® Assessment Report**

## **Initial Assessment**

VIMERCATI SPA

SK75YZ

AV80AN-1

09.08.2024

Version 1

## Initial Remarks

This Assessment Report and its underlying assessment was created by qualified experts of an TISAX audit provider. It expresses professional judgement of the effectiveness of control procedures based on the current state of implementation and in accordance to the Audit Provider Criteria and Assessment Requirements (ACAR) of the Trusted Information Security Assessment Exchange (TISAX) as defined and published by ENX Association at the time of the issuance of this report.

The Trusted Information Security Assessment Exchange (TISAX) is operated and governed by ENX Association. TISAX was created to provide commonly accepted assessments based on the ISA control catalogue conducted by trustworthy competing audit providers. Detailed information about TISAX can be found at <http://www.enx.com/tisax/>.

This Assessment Report is intended exclusively for use within TISAX. All distribution or exchange of TISAX Assessment Results must follow the rules for information exchange established for TISAX Participants and TISAX Audit Providers within the applicable TISAX agreements and guidelines.

No exchange of TISAX Assessment Results outside the defined TISAX information exchange proceedings or exchange with third parties outside the TISAX shall take place. Please be aware that certain rights provided by the applicable TISAX legal framework may cease when exchanging TISAX Assessment Results outside the set guidelines.

The underlying assessment engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the checks performed on the control procedures are on a sample basis. As such, even though checks are conducted with due diligence, misstatements due to errors or fraud may occur and go undetected.

Additionally, the assessment was based on the situation at the day of the assessment and does not account for any changes in the future. Any projections of any evaluation to future periods are subject to the risk that the report may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate.

## Report Structure

This report is structured as follows:

- A. Assessment Related Information
- B. Summarized Results
- C. Assessment Result Summary
- D. Maturity Levels of ISA (Result Tab)
- E. Detailed Assessment Results

The structure and headlines reflect different levels of possible disclosure regarding its content towards other TISAX Participants.

Starting with general information about the assessment (A. Assessment-Related Information), it spans from a summary of results (B. Summarized Results, C. Assessment Result Summary) to the very details of the assessment (D. Maturity Levels of ISA and E. Detailed Assessment Results).

## A. Assessment Related Information

### A.1 Assessment Scope

<b>TISAX® Scope-ID</b>	SK75YZ
<b>Scope Type</b>	<input checked="" type="checkbox"/> Standard Scope 2.0 <i>The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.</i>  <i>The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.</i>  <input type="checkbox"/> Custom Extended Scope  <input type="checkbox"/> Full Custom Scope
<b>Assessment Objectives</b>	<input type="checkbox"/> Handling of Information with High Protection Level <input checked="" type="checkbox"/> Handling of Information with Very High Protection Level <input checked="" type="checkbox"/> Handling of Prototype Components and Parts <input type="checkbox"/> Handling of Prototype Vehicles <input type="checkbox"/> Use of Test Vehicles <input type="checkbox"/> Events and Photo Shootings with Objects in Need of Protection <input checked="" type="checkbox"/> Handling of Personal Data according to article 28 GDPR ("processor") <input type="checkbox"/> Handling with Special Categories of Personal Data (article 9 GDPR) according to article 28 GDPR ("processor")
<b>Assessment Requirements</b>	ACAR – TISAX Specification of Assessment Version 2.1: Family-ID: ISA, Version 5.0

### A.2 Assessed Locations

Company Name	Address	Location-ID	Contact Person
<b>VIMERCATI SPA</b>	Via Vincenzo Monti, 38 - 20016 Pero (MI)		Roberto Ferrari roberto.ferrari@vimercati.com

The auditor confirms that all information above is verified to be accurate.

### A.3 Initial Assessment

<b>TISAX® Assessment-ID</b>	AV80AN-1
<b>Assessment Level</b>	AL3
<b>Assessment Method</b>	<input checked="" type="checkbox"/> Plausibility check of self-assessment using evidences and documentation <input checked="" type="checkbox"/> Detailed evaluation of evidence <input checked="" type="checkbox"/> Interviews with persons involved in the processes of the auditee <input checked="" type="checkbox"/> On-site Inspection <input type="checkbox"/> Video based remote site inspection
<b>Date of Kick-Off Meeting</b>	19.07.2024
<b>Date of Opening Meeting</b>	07.08.2024
<b>Date of Closing Meeting (Effective Date)</b>	09.08.2024
<b>Consent of Auditee</b>	The auditee <input checked="" type="checkbox"/> unqualifiedly agrees on the documented conclusions. <input type="checkbox"/> qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

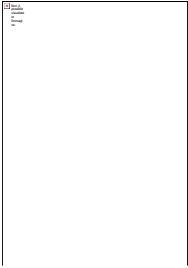
### Authors

<b>Auditor</b>
Maurizio Genna
<b>Quality Assurance</b>
Bureau Veritas Italia SpA

Pero, 09.08.2024

Maurizio Genna

Roberto Ferrari



Signature

## B. Summarized Results

### B.1 Initial Assessment

AL3: Based on the observations during the initial assessment the overall assessment of the scope is:

- ☒ Conform
- ☐ Minor non-conform (only minor non-conformities exist)
  - ☐ Minor non-conformities without defined corrective actions exist.
  - ☐ All minor non-conformities have defined corrective actions. Latest corrective action is due on yyyy-mm-dd (temporary labels may be issued until this date).
  - ☐ A video supported remote assessment method has been conducted and an on-site inspection has been scheduled as part of corrective actions.
  - ☐ The overall maturity level is more than 10% below the target maturity level (<2,7).
- ☐ Major Non-conform
  - ☐ Some of the non-conformities create immediate significant risks, in addition to a suitable corrective action plan, compensating measures must be implemented before the status can change to "Minor Non-conform"
  - ☐ The overall maturity level is more than 30% below the target maturity level (<2,1).

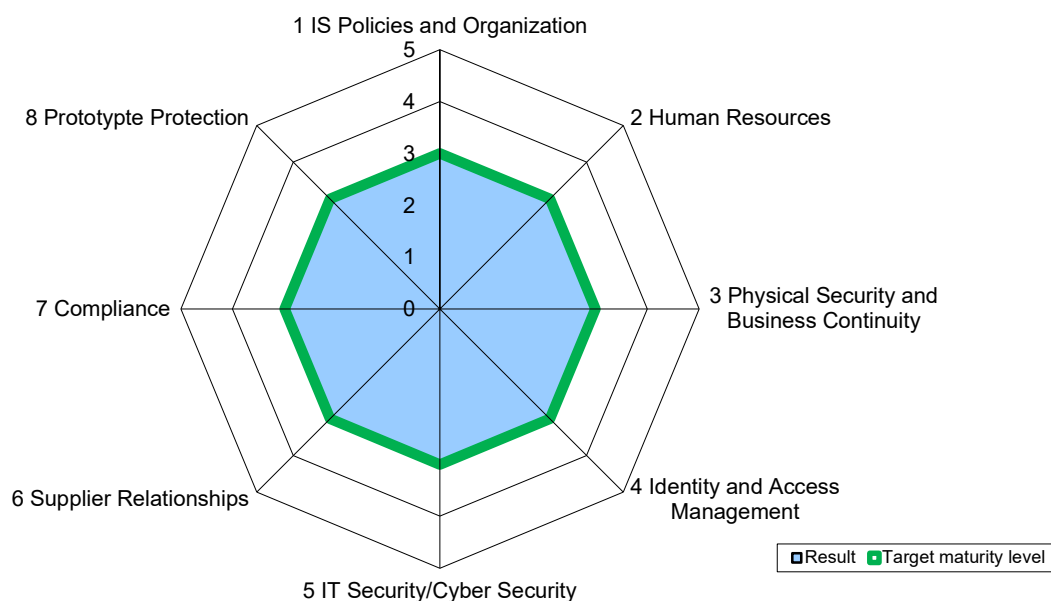
In total, {0} major and {0} minor non-conformities to the assessed catalogue were identified.

After the initial assessment an average maturity level of 3,00 was calculated.

## C. Assessment Result Summary

### C.1 Initial Assessment

The individual areas of the initial maturity levels can be found in the spider web diagram below.



The major and/or minor non-conformities, as applicable, were identified in the following Areas:

No.	Area	Number of major non-conformities	Number of minor non-conformities
1	IS Policies and Organization	0	0
2	Human Resources	0	0
3	Physical Security and Business Continuity	0	0
4	Identity and Access Management	0	0
5	IT Security / Cyber Security	0	0
6	Supplier Relationships	0	0
7	Compliance	0	0
8	Prototype Protection	0	0
9	Data Protection	0	0

## D. Maturity Levels of ISA (Result Tab)

### D.1 ISMS

Based on the current status of implementation, the following maturity levels result for the controls listed in the ISMS Area:

No.	Control Question	Target maturity level	Result
1	<b><i>IS Policies and Organization</i></b>		
1.1	<b><i>Information Security Policies</i></b>		
1.1.1	To what extent are information security policies available?	3	<b>3</b>
1.2	<b><i>Organization of Information Security</i></b>		
1.2.1	To what extent is information security managed within the organization?	3	<b>3</b>
1.2.2	To what extent are information security responsibilities organized?	3	<b>3</b>
1.2.3	To what extent are information security requirements taken into account in projects?	3	<b>3</b>
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	<b>3</b>
1.3	<b><i>Asset Management</i></b>		
1.3.1	To what extent are information assets identified and recorded?	3	<b>3</b>
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	<b>3</b>
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	<b>3</b>
1.4	<b><i>IS Risk Management</i></b>		
1.4.1	To what extent are information security risks managed?	3	<b>3</b>
1.5	<b><i>Assessments</i></b>		
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	<b>3</b>
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	<b>3</b>
1.6	<b><i>Incident Management</i></b>		
1.6.1	To what extent are information security events processed?	3	<b>3</b>



2	<b>Human Resources</b>		
2.1.1	To what extent is the suitability of employees for sensitive work fields ensured?	3	<b>3</b>
2.1.2	To what extent is all staff contractually bound to comply with information security policies?	3	<b>3</b>
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	3	<b>3</b>
2.1.4	To what extent is teleworking regulated?	3	<b>3</b>
3	<b>Physical Security and Business Continuity</b>		
3.1.1	To what extent are security zones managed to protect information assets?	3	<b>3</b>
3.1.2	To what extent is information security ensured in exceptional situations?	3	<b>3</b>
3.1.3	To what extent is the handling of supporting assets managed?	3	<b>3</b>
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	3	<b>3</b>
4	<b>Identity and Access Management</b>		
4.1	<b>Identity Management</b>		
4.1.1	To what extent is the use of identification means managed?	3	<b>3</b>
4.1.2	To what extent is the user access to network services, IT systems and IT applications secured?	3	<b>3</b>
4.1.3	To what extent are user accounts and login information securely managed and applied?	3	<b>3</b>
4.2	<b>Access Management</b>		
4.2.1	To what extent are access rights assigned and managed?	3	<b>3</b>
5	<b>IT Security/Cyber Security</b>		
5.1	<b>Cryptography</b>		
5.1.1	To what extent is the use of cryptographic procedures managed?	3	<b>3</b>
5.1.2	To what extent is information protected during transport?	3	<b>3</b>
5.2	<b>Operations Security</b>		
5.2.1	To what extent are changes managed?	3	<b>3</b>

5.2.2	To what extent are development and testing environments separated from operational environments?	3	3
5.2.3	To what extent are IT systems protected against malware?	3	3
5.2.4	To what extent are event logs recorded and analyzed?	3	3
5.2.5	To what extent are vulnerabilities identified and addressed?	3	3
5.2.6	To what extent are IT systems technically checked (system audit)?	3	3
5.2.7	To what extent is the network of the organization managed?	3	3
5.3	<b><i>System acquisitions, requirement management and development</i></b>		
5.3.1	To what extent is information security considered in new or further development of IT systems?	3	3
5.3.2	To what extent are requirements for network services defined?	3	3
5.3.3	To what extent is the return and secure removal of information assets from external IT services regulated?	3	3
5.3.4	To what extent is information protected in shared external IT services?	3	3
6	<b><i>Supplier Relationships</i></b>		
6.1.1	To what extent is information security ensured among suppliers and cooperation partners?	3	3
6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	3	3
7	<b><i>Compliance</i></b>		
7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?	3	3
7.1.2	To what extent is the protection of personal data taken into account when implementing information security?	3	3

## D.2 Handling of Prototypes

Based on the current status of implementation, the following maturity levels result for the controls listed in the Prototype Protection area:

No.	Control Question	Target maturity level	Result
8.1	<b><i>Physical and Environmental Security</i></b>		
8.1.1	Security concept	3	3

8.1.2	Perimeter security	3	3
8.1.3	Stability of outer skin	3	3
8.1.4	View and sight protection	3	3
8.1.5	Protection against unauthorized entry and access control	3	3
8.1.6	Intrusion monitoring	3	3
8.1.7	Visitor management	3	3
8.1.8	Client segregation	3	3
8.2	<b>Organizational Requirements</b>		
8.2.1	Non-disclosure obligations	3	3
8.2.2	Subcontractors	3	3
8.2.3	Awareness	3	3
8.2.4	Security classification	3	3
8.2.5	Access control	3	3
8.2.6	Film and photo regulations	3	3
8.2.7	Mobile video and photography devices	3	3
8.3	<b>Handling of vehicles, components and parts</b>		
8.3.1	Transport	3	3
8.3.2	Parking and storage	3	3
8.4	<b>Requirements for trial vehicles</b>		
8.4.1	Camouflage	3	n.a.
8.4.2	Test and trial ground	3	n.a.
8.4.3	Test and trial drives on public roads	3	n.a.
8.5	<b>Requirements for events and shootings</b>		
8.5.1	Presentations and events	3	n.a.
8.5.2	Film and photo shootings	3	n.a.

### D.3 Data Protection

The Data Protection Module is not following the ISA maturity levels and therefore not listed here.

## E. Detailed Assessment Results

### 1 IS Policies and Organization

#### 1.1 Information Security Policies

##### 1.1.1 To what extent are information security policies available?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>VIMERCATI Company Policy, revised on 2022, listing overall guidelines including information security points. An additional Corporate Social responsibility Policy for ESG sustainability is defined and applied.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Company Policy, Rev.4, 28/10/2022</li><li>• Corporate Social Responsibility Policy, Dec/2022</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

1.2 Organization of Information Security

1.2.1 To what extent is information security managed within the organization?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Information Security Management System in place in Vimercati with resources, processes/procedures, target, actual KPI</p> <p>The Management identifies strategic processes with which to achieve information security objectives in all company activities in support of its Customers, processes that are collected in a real Information Security Management System (ISMS).</p> <p>Management review: dated 11/1/2024 + company dashboard</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Riesame Direzione, Jan/2024</li><li>• Organization chart, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found, but <b>improve the analysis of KPIs-objectives-change on the Tisax side in the next management review.</b></p>
Planned measures (including implementation period)
Evaluation at Follow-Up

1.2.2 To what extent are information security responsibilities organized?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Responsibilities for the information security within the organization are defined, documented and assigned according also other Certification Standards.</p> <p>The responsible employees are defined and qualified for their task.</p> <p>The contact persons are known within the organization and to relevant business partners. An appropriate organizational separation of responsibilities should be established in order to avoid conflict of interests.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Organization chart, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

1.2.3 To what extent are information security requirements taken into account in projects?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Information security requirements listed in Information Security Rules document</p> <p>Information classification: public-internal and confidential. All data on server. Folder access for Groups, there are no teams dedicated to Customers. Project: PM carries out an evaluation triggered by the salesperson to carry out feasibility analysis with all the technical functions, solution evaluation and time and costs. Cardinis (sw management) for planning management + PDMLink for deliverables (drawings, models, test records and product documentation).</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

1.2.4 To what extent are responsibilities between external IT service providers and the own organization defined?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>The IT services subject to external supplies are listed and classified based on their actual relevance and security requirements.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up



1.3 Asset Management

1.3.1 To what extent are information assets identified and recorded?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>The information assets of the following categories are identified:</p> <ul style="list-style-type: none"><li>- IT hardware and applications;</li><li>- IT-supporting infrastructure;</li><li>- information in electronic form, in paper form and physical form;</li><li>- individual and groups of persons holding relevant information</li><li>- outsourced services.</li></ul> <p>Each information asset is assigned to a responsible entity (individual or organizational unit).</p> <p>Information assets are classified.</p> <p>Information asset inventories are prepared and updated regularly.</p> <p>Asset management (server) within Nagios.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information assets list, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

1.3.2 To what extent are information assets classified and managed in terms of their protection needs?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Know-how protection: defined different security levels based on the information contents.</p> <p>A consistent scheme for the classification of documents/information is in place and implemented.</p> <p>Classification of information is done according to defined criteria, e.g. customer requirements, confidentiality, integrity and availability.</p> <p>A policy including requirements for classification of information as well as the respective protective measures for identification, handling, transfer, storage, deletion and disposal is in place and implemented.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**1.3.3 To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?**

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>For each external IT service, analysis of information security requirements is carried out, suppliers were assessed and contracts include legal and regulatory requirements to ensure harmonization with the information assets protection needs.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Service contracts</li><li>• Risk evaluation</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

1.4 IS Risk Management

1.4.1 To what extent are information security risks managed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Risk assessments can be performed regularly, there is a risk assessment document that documents and assesses information security risks. For each potential risk, a person is assigned who is responsible for assessing the risk and implementing risk mitigation and management policies.</p> <p>Risk analysis: analysis view of system KPIs (SLA - incidents - incident costs - training - PC with antivirus protection - information asset mapping - user updates) with a three-year history. OS ticketing for request management with SLA monitoring. Improvement of data loss prevention – segregation – back up – MFA – mobile – regulations/laws.</p> <p>Verified risk analysis 2024 with some risk over threshold and related treatment plan.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>ISMS KPI &amp; Risk</li><li>M009 - M038 Risk analysis forms</li></ul>
Finding
<p>Based on the observations, no deviation was found, but <b>It is recommended to review the risk analysis to integrate current threats/vulnerabilities with those present in databases.</b></p>
Planned measures (including implementation period)
Evaluation at Follow-Up

## 1.5 Assessments

### 1.5.1 To what extent is compliance with information security ensured in procedures and processes?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Procedures defined and applied for ISMS.</p> <p>Each document has a manager and review. The technical specifications are reviewed annually.</p> <p>All changes are communicated to users through the appropriate communication channels.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>List of Procedures &amp; Modules in QHSE repository</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

1.5.2 To what extent is the ISMS reviewed by an independent entity?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>TISAX assessment regularly performed</p> <p>The documents are validated by fast bit during new revisions and periodically during the renewal of certifications (TISAX).</p> <p>Internal audit: on VDA check list on 07/20/2024 with verification of some points of the system.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• M032 Audit program</li><li>• Audit report</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

## 1.6 Incident Management

### 1.6.1 To what extent are information security events processed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>A risk analysis has been carried out based on the company structure, and measures have been adopted to mitigate the risks: always have the continuous update of vulnerabilities in order to be able to intervene and apply the mitigation procedures (patches). procedure for managing the loss of company tools (e.g. PCs) and avoid access and theft of company data. Intrusion tests are periodically carried out to test the security of the company perimeter. It is also possible to have feedback on any vulnerabilities and problems through reports that can be made by users via the ticketing system (OSTicket)</p> <p>Security incidents none – only events that did not result in data loss.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Risk analysis</li><li>• VA &amp; PT report</li><li>• Information Security Rules</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

## 2 Human Ressources

### 2.1.1 To what extent is the suitability of employees for sensitive work fields ensured?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Defined expected levels of competence and knowledge for IT employee.</p> <p>Job description are defined according ISO 9001.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Job descriptions VIMERCATI</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up



**2.1.2 To what extent is all staff contractually bound to comply with information security policies?**

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>NDA signed by each employee</p> <p>Induction plan provided by HR + meetings with management managers (Usage regulations + temporary passwords to be updated every 3 months for both domain and SAP). Confidentiality: NDA signed by employee.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• NDA document at Personnel Office</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

2.1.3 To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Training for new employee are constantly performed</p> <p>Training: verified training plan 2024-2025; initial training during the induction phase of new hires also on cyber security issues; seen training on 14 front line people + extension expected in September with 3 sessions. Seen data processing module + company data processing (confidentiality)</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Company training plan, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found, but <b>It is recommended to re provide phishing sessions to improve staff awareness.</b></p>
Planned measures (including implementation period)
Evaluation at Follow-Up

#### 2.1.4 To what extent is teleworking regulated?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>The use of mobile devices (e.g. smartphones, notebooks) is subject to regulation. A policy is prepared considering the following aspects:</p> <ul style="list-style-type: none"><li>- Registration of mobile devices</li><li>- Physical protection requirements (among others against theft, spying on information)</li><li>- Software installation restrictions</li><li>- Requirements for the versioning of software for mobile devices and the associated patch management</li><li>- Limitations of access to certain information services</li></ul> <p>Users sign an obligation declaration regarding the handling of particularities when working with mobile devices depending on the protection needs.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Smartworking policy</li><li>• VPN procedure</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

### 3 Physical Security and Business Continuity

#### 3.1.1 To what extent are security zones managed to protect information assets?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Inside the Company all prototyping areas and CED rooms have controlled access via Badge. All company personnel are aware of which areas are sensitive and have limited access. There are procedures that define the access methods to the various areas. Access protection of personal company devices (PCs) is managed through company policies that define the type of access based on the function and department of the individual person.</p> <p>Checked two server rooms in two different buildings, badge access, in the primary UPS/air conditioner/2 racks - in the secondary air conditioner 1 rack.</p> <p>Laboratory (4) where the prototypes are managed during their life cycle are closed with access via badge; are UT-Purchases-quality access monitored by cameras.</p> <p>Layout: CCTV + alarm system connected to the Surveillance Institute which remotely enables and disables access. In production with talking coding. Shipping to customer specification with packaging that can be organized by Vimercati or picked up by the customer, with recyclable or disposable customer packaging.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"> <li>• Procedure P208 - Prototyping areas access procedure for defining access to restricted areas through additional authorizations.</li> <li>• Procedure P318 External personnel access procedure for the access policy for general visitors.</li> <li>• Procedure P201 -User management procedure for managing access authorizations to the network/company resources.</li> </ul>
Finding
Based on the observations, no deviation was found, but <b>It is recommended to monitor the temperature in the primary data center.</b>
Planned measures (including implementation period)
Evaluation at Follow-Up

### 3.1.2 To what extent is information security ensured in exceptional situations?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Referring to SAP: the management of exceptional events, since the system is in the cloud, is delegated to the service providers themselves: SAP/AWS. They must ensure the redundancy and high reliability of the systems. In SAP, backups are still carried out to guarantee the saving and possible restoration of the data contained in the database.</p> <p>Referring to IT infrastructure, Firewalls and antivirus systems are configured to detect any attacks and notify them; once notified, the procedure for controlling, mitigating or eliminating the threat starts</p> <p>Back ups managed with Veeam v.12.2.5 (2 servers), one (layer) performs normal functionality with snapshots with 5 days of retention + 2nd back up on deduplication system which also saves at midday, 3rd layer and 4th Hyden back up layer with unreachable deduplication system and data replication in DC in Caldera.</p> <p>Layer – non-backup storage;</p> <p>Layer 1: daily incremental at 11.59pm - full Saturday 1 week of retentions; CED</p> <p>Layer 2: midday – 30 days; secondary room full on Sunday;</p> <p>Layer 3; daily incremental to 8pm</p> <p>Layer 4: Synchronization with DC in real time.</p> <p>Verified back up restore report on 3rd layer JDOC machine, with selected restore points created on another virtual machine without final power-on. RTO 6-8 hours if damage is not to the building.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"> <li>• SAP procedures</li> <li>• Procedure P202 System backup</li> </ul>
Finding
Based on the observations, no deviation was found, but <b>Improve back restore/DR planning to cover all layers and increase restore depth.</b>
Planned measures (including implementation period)
Evaluation at Follow-Up

3.1.3 To what extent is the handling of supporting assets managed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>A company procedure is established for the management of cases of loss/misplacement of company accesses rather than company tools (PCs), once the problem is notified, the procedure for closing accesses starts in order to reduce the risk to company security to a minimum. Procedures are also established for the safe disposal of company devices. For example, the PC disk is made unusable or the data is safely deleted</p> <p>Decommissioned or reused PCs: PC rented with the possibility of decommissioning (machine reset and installation re-installed if reused); if destined for destruction, the HD is cleaned or destroyed. Bitlocker installed on server and client.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information Security Rules, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

3.1.4 To what extent is the handling of mobile IT devices and mobile data storage devices managed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>All PCs are encrypted to ensure data protection. Strongly protected access to company premises. Corporate VPN access with multi-factor self-attentication for external access. Smartphones do not have access to the company network and only manage mail. As a policy, company data must be saved only on the network shares made available.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li><li>• Information Security Rules, July/2024</li><li>• (including company policy about backup and device usage)</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

## 4 Identity and Access Management

### 4.1 Identity Management

#### 4.1.1 To what extent is the use of identification means managed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>The user for access to computer systems can be:</p> <ul style="list-style-type: none"><li>a) Basic User: is the user uniquely associated with a natural person, enabled for access to common IT tools and equipment in general;</li><li>b) Application User: is the user uniquely associated with a natural person, through which the subject is recognized by an application or program and is enabled to use specific application functions, linked to his role within the complex structure of which it is part.</li></ul> <p>The user, with regard to Active Directory systems, can be:</p> <ul style="list-style-type: none"><li>a) User: can access the computer system and its database (if applicable) and can enter new information, and modify and save existing ones based on the privileges granted by the administrator;</li><li>b) Power User: can perform, in addition to all the activities foreseen for the User user, checks in reading only of the information contained in the information assets, using</li><li>c) advanced features such as the recovery of records necessary for it activitiesverify;</li><li>d) Administrator: can perform, in addition to all the activities foreseen for the Power User, the activity of assigning and modifying privileges, resetting the machines given in use to the users (by modifying or adding software) and check user log files;</li><li>e) Guest: is the external party who receives a temporary User account with which he can access the computer system in read-only mode. He is not authorized to modify theexisting records.</li></ul> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• For network access they use company name accounts, for physical access they use company personal badges</li><li>• Demonstration in-the-field</li></ul>
Finding
Based on the observations, no deviation was found.



Planned measures (including implementation period)
Evaluation at Follow-Up

**4.1.2 To what extent is the user access to network services, IT systems and IT applications secured?**

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Authentication procedures are implemented following the security criteria defined by the company and evaluating the possible risks. An Active Directory system is used for user management and their authentication and control, complete procedures are defined for user management: creation, assignment, modification, disabling and deletion.</p> <p>VPN – double factor on external device with Google authenticator; office 365 account with nominal account. MFA to VPN possible on all Microsoft; have Rubric for internal ADS authentication.</p> <p>DLP: Libraesva which verifies protected source (not very flexible) + TrendMicro for USB port management (antivirus and EDR with access block).</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li><li>• Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found, but <b>It is recommended to extend MFA coverage to all users as soon as possible, as per the improvement plan and better ). Improve the management of automatic functions typical of more advanced DLP systems (currently the policies and tools used provide adequate coverage).</b></p>
Planned measures (including implementation period)
Evaluation at Follow-Up

4.1.3 To what extent are user accounts and login information securely managed and applied?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>There is a procedure that manages the users, starting from the authorized request, we proceed to the creation, to the assignment of the various authorizations, passing through the possible modification (change of job or role) and finally to the disabling and then deletion of the user itself. every 6 months the user control procedure is carried out. the assigned passwords are temporary and at the first access a change is requested. there are password complexity rules and instructions in the event of loss or potential compromise of the password.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li><li>• Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

4.2 Access Management

4.2.1 To what extent are access rights assigned and managed?

<p><b>Detailed Description (Including Assessment Procedure)</b></p> <p>AL3. Considered documents/evidences/audit trail:</p> <p>There is a procedure that manages the users, starting from the authorized request, we proceed to the creation, to the assignment of the various authorizations, passing through the possible modification (change of job or role) and finally to the disabling and then deletion of the user itself.</p> <p>Phases defined and managed in the procedure :</p> <p>a) Creation: user activation phase and subsequent release of the appropriate credentials and access privileges;</p> <p>b) Reset: user reset request phase and subsequent sending of new access credentials (eg temporary password);</p> <p>c) Modification: request phase for a change in user privileges and implementation of this change;</p> <p>d) Disabling: phase of deactivation of user access privileges and cancellation of the user itself (in cases of interruption of the employment relationship, end of a mandate /assignment, etc.);</p> <p>e) Periodic review: phase of verification of the conditions that justify the allocation of users and the correspondence of the privileges associated with the access profiles issued; the periodic review of utilities starting from the list updated by HR and carried out verification. EDR can check dormant users and verify clients registered in the domain who have not authenticated for at least 90 days.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li><li>• Information Security Rules, July/2024</li><li>• Samples of creation/cancellatio/periodic review.</li></ul>
<p><b>Finding</b></p> <p>Based on the observations, no deviation was found.</p>
<p><b>Planned measures (including implementation period)</b></p>
<p><b>Evaluation at Follow-Up</b></p>

5 IT Security / Cyber Security

5.1 Cryptography

5.1.1 To what extent is the use of cryptographic procedures managed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>PCs are encrypted with solutions compliant with standard protocols and state-of-the-art procedures. The file classification criteria are defined and based on these the most suitable encryption systems for their security and movement are established.</p> <p>VPN – double factor on external device with Google authenticator; office 365 account with nominal account. MFA to VPN possible on all Microsoft; have Rublic for internal ADS authentication.</p> <p>Bitlocker installed on server and client.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

5.1.2 To what extent is information protected during transport?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>The transfer of confidential files occurs exclusively through secure and encrypted SFTP/SCP protocols, the methods, protocols and programs used for such transfers are classified and known.</p> <p>Document transmission: SFTP server, encrypted protocol and software (Filezilla= to configure transfer logs) Technical office-Purchasing office.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information Security Rules, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2 Operations Security

5.2.1 To what extent are changes managed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Any existing and new role is mapped in terms of information security.</p> <p>Full MFA coverage and new DLP projects are currently open.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.2 To what extent are development and testing environments separated from operational environments?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Electronic software development + electronic cards for the test phase + machine engineering</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P202 Systems backup, May/2024</li><li>• 'Information security rules - May2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up



### 5.2.3 To what extent are IT systems protected against malware?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Malware risks have been assessed. Trend Micro's centralized anti-malware antivirus system is used, configured so that it cannot be deactivated by the user. Incoming email is checked with the Libraesva system. Only IT administrators can install or uninstall SW and requests for new SW are assessed by IT based on Vimercati's security criteria. Any incidents are immediately identified and reported to IT so that their dangerousness can be assessed and mitigation and safety actions can be undertaken. Staff is trained and updated to mitigate human error aspects.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P206 Antispam e SandBox</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.4 To what extent are event logs recorded and analyzed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Systems include automatic logging technology, where possible security-relevant logs are sent to administrators who analyze risks, assess critical issues and prepare systems for mitigation and resolution of events.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information security rules - May2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.5 To what extent are vulnerabilities identified and addressed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Asset administrators are constantly notified of detected vulnerabilities and regularly perform vulnerability tests on the systems. Based on the test results and information received, vulnerable systems are identified and patched where already available or mitigation and security procedures are implemented if a definitive solution to the vulnerability is not available.</p> <p>Patching – VA-PT: WSUS automatically releases patches either from the network or the internet – manual server. Nessus for the part of VA-PT of November 2023 external for public IPs with some reports on the manager's router (some on pre office 365 - router manager).</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information security rules - May2024</li></ul>
Finding
Based on the observations, no deviation was found, but <b>It is recommended to implement a continuous VA system or increase the frequency of VA.</b>
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.6 To what extent are IT systems technically checked (system audit)?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Vulnerability tests are performed on systems based on specifications and state of the art, the test results are used to develop containment, mitigation and security measures. The test results are available.</p> <p>Monitoring: Nagios – infrastructure audit report with capacity-availability-back up. Nagios dashboard view with the various monitoring settings.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information security rules - May2024</li><li>• Network diagrams - May2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**5.2.7 To what extent is the network of the organization managed?**

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Requirements for segmenting the company network are identified based on the security criteria imposed by the corporate policy and the Information Security rules; networks are segmented to ensure the security of information. There are no active connections between the company network and the one of the customers. Lines assigned to visitors are separated from the company network and the devices are segregated.</p> <p>Verified network diagram - infrastructure based on active directory with two domain controllers with password management policy which also manages wi-fi. Networks managed by one core in the data center, the second core in the second building with another room with back up and part of the network. Switch in the two departments subject to policies of the two cores under Cisco HA firewall with navigation control, barracuda acting as proxy for calls passing through the firewall. 4 connections with double (fiber + back up); SAP with double VPN on AWS to also manage failures to and from AWS and vice versa. VLAN with policies applied on firewall (Client-Server - 2 back up - 2 production - internal WI-FI network - Guest wi-fi network - machinery network for mac address control (guns....). VMware vSphere with HA machines HP that automatically manage virtual machine failover. Each machine has double electrical connections on two UPSs (5,000+5,000).</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information security rules - May2024</li><li>• Network diagrams - May2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

5.3. System acquisitions, requirement management and development

5.3.1 To what extent is information security considered in new or further development of IT systems?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Information security requirements are listed and checked in the development or acquisition of IT systems.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information security rules - May2024</li><li>Network diagrams - May2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

5.3.2 To what extent are requirements for network services defined?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Information security requirements are listed and checked in the development or acquisition of IT systems.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>Information security rules - May2024</li><li>Network diagrams - May2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**5.3.3 To what extent is the return and secure removal of information assets from external IT services regulated?**

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>IT assets managed during their life-cycle</p> <p>Cloud service applied in Vimercati: Office 365 – SAP – email in DC – personal management.</p> <p>Information data retention and secure removal are managed contractually with the external Provider.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P203 Asset management</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up



**5.3.4 To what extent is information protected in shared external IT services?**

<b>Detailed Description (Including Assessment Procedure)</b>
AL3. Considered documents/evidences/audit trail:  The information managed by external providers is regulated by contract and contractual technical conditions between Vimercati and the Provider.  The following evidences were provided: <ul style="list-style-type: none"><li>• Procedure P201 users management</li></ul>
<b>Finding</b>
Based on the observations, no deviation was found.
<b>Planned measures (including implementation period)</b>
<b>Evaluation at Follow-Up</b>

6 Supplier Relationships

6.1.1 To what extent is information security ensured among suppliers and cooperation partners?

<b>Detailed Description (Including Assessment Procedure)</b>
<p>AL3. Considered documents/evidences/audit trail:</p> <p>All suppliers are assessed for security; everyone is made to sign the non-disclosure document and the contract contains all the security levels that must be respected. Eventually the supplier must also respect the security levels, if it is requested by Vimercati customers. once authorized, a badge is assigned for physical access to the various areas and credentials for access to the network and company resources.</p> <p>Suppliers: plastic component molding - painting and chrome plating. The supply specifications (rev. 7 dated 06/10/2023) have been sent to all suppliers, indicating confidentiality terms and security requirements (see specifications signed by Progind which prints plastic components).</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules - May2024</li><li>• NDA with suppliers</li><li>• Contracts with suppliers</li></ul>
<b>Finding</b>
Based on the observations, no deviation was found.
<b>Planned measures (including implementation period)</b>
<b>Evaluation at Follow-Up</b>

6.1.2 To what extent is non-disclosure regarding the exchange of information contractually agreed?

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Any supplier is requested to sign for approval the supply specificatiopn document, including information exchange (referred to valid regulations and laws)</p> <p>Verified Portguardian.com contract of January 2024 IT supplier for server system support - firewall...SLA + letters dated 09/01/2023 treatment and system administrator of the 3 Portguardian technicians.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• SSPEC Supply specification - Oct2023</li></ul>
Finding
Based on the observations, no deviation was found, but <b>better improve, in the contract with the IT supplier, the definition of the SLAs for ordinary and extraordinary assistance.</b>
Planned measures (including implementation period)
Evaluation at Follow-Up

7 Compliance

7.1.1 To what extent is compliance with regulatory and contractual provisions ensured?

Detailed Description (Including Assessment Procedure)
AL3. Considered documents/evidences/audit trail:  Periodical check of regulatory and legal requirements done  The following evidences were provided: <ul style="list-style-type: none"><li>• Communication from Personnel</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**7.1.2 To what extent is the protection of personal data taken into account when implementing information security?**

Detailed Description (Including Assessment Procedure)
<p>AL3. Considered documents/evidences/audit trail:</p> <p>Personal data protection aligned to GDPR regulation and Viemrcati policies</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Viemrcati Organisational model - Dec2023</li><li>• Code1-Of_Ethics - Sept2023</li><li>• GDPR regulations</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8 Prototype Protection

8.1 Physical and Environmental Security

8.1.1 To what extent is a security concept available describing minimum requirements regarding the physical and environmental security for prototype protection?

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>Vimercati has adopted protection criteria for both the Information Security and Physical Security prototypes. All data relating to prototypes are considered confidential and processed according to the procedures established by the IT Security Regulation, which is delivered to each employee and used for training. Vimercati has implemented specific procedures for the physical safety of the prototypes which concern: - the management of authorizations and access to the premises and the access register - the masking and packaging of the prototypes - the authorizations and transport of the prototypes - the physical safety of the rooms and the segregation of environments</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

8.1.2 To what extent is perimeter security existent preventing unauthorized access to protected property objects?

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>Access to Vimercati is manned and external visits must be authorised, each visitor is identified and registered. access to the Prototyping areas is protected by a system of manned gates, the authorization procedure is defined and known and involves the activation of a badge to open the gates. Accesses are recorded.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.1.3 To what extent is the outer skin of the protected buildings constructed such as to prevent removal or opening of outer-skin components using standard tools?**

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>The Vimercati buildings are solidly built with concrete walls, protected but masonry fences and steel gates; the production itself manages the prototypes with controlled access.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Company planimetry</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up



8.1.4 To what extent is view and sight protection ensured in defined security areas?

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>The windows and glass panels in the areas dedicated to prototyping are designed so as not to allow unauthorized viewing.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.1.5 To what extent is the protection against unauthorized entry regulated in the form of access control?**

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>There are two lines of control: - Access to the Vimercati building with authorization, identification and register. - Access to the prototyping rooms through manned gates with electronic control and via personal badge with registration authorization.</p> <p>The access gates to the Prototyping areas are protected by electronic access devices, access is authorized by means of a Badge. Employees who by role or function are authorized to access the areas receive the badge already configured, staff who, due to a change in role or function, receive authorization to access the reserved areas will have their badge updated with the new authorizations, upon termination of access needs and therefore the revocation of authorizations, the badge will be disabled or updated with the new authorizations.</p> <p>Temporary badges may be issued, upon request supported by feedback and authorization, to suppliers and customers for the time necessary for the activities defined in the request, at the end of which the authorizations will be revoked.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.1.6 To what extent are the premises to be secured monitored for intrusion?**

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>Intrusion detection implemented out of working hours period. During working hours, checks are carried out by internal staff, after working hours by external security company.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Contratto con security company</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.1.7 To what extent is a documented visitor management in place?**

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>External personnel who need to access the company must report to the switchboard or the receipt of goods and follow the instructions for registration on the appropriate portal</p> <p>Kereception by Vimercati staff, receive the relevant 'guest' badge and wait for reference company personnel.</p> <p>Visitor management: reception - accompanied - dedicated rooms.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P318 External personnel access procedure for the access policy for general visitors.</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8.1.8 To what extent is on-site client segregation existent?

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>Customer segregation is mainly implemented by keeping the customer on visits outside the prototyping departments. Only in the case of an equipment inspection visit is the customer authorized to access, accompanied and all material not subject to inspection/visit segregated. designated areas.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P318 External personnel access procedure for the access policy for general visitors.</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

8.2 Organizational Requirements

8.2.1 To what extent are non-disclosure agreements/obligations existent according to the valid contractual law?

Detailed Description (Including Assessment Procedure)
<p>Considered documents/evidences/audit trail:</p> <p>For each contract, an NDA is prepared and signed in compliance with current laws. Each employee is given a copy of the IT Security Regulations and has access to the security regulations and procedures and must sign the NDA</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Procedure P201 User management, June/2024</li><li>• Information Security Rules, July/2024</li><li>• NDA</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.2.2 To what extent are requirements for commissioning subcontractors known and fulfilled?**

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>For each subcontracting contract, an NDA compliant with the law is prepared and signed.</p> <p>Molding of plastic components - painting and chrome plating. The supply specifications (rev. 7 dated 06/10/2023) have been sent to all suppliers, indicating confidentiality terms and security requirements (see specifications signed by Progind which prints plastic components).</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• 'Procedure P318 External personnel access procedure for the access policy for general visitors.</li><li>• NDA</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8.2.3 To what extent do employees and project members evidently participate in training and awareness measures regarding the handling of prototypes?

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Every employee receives the IT security regulation upon joining the company and has access to the security regulations, manuals and procedures for which he is responsible. Training is carried out throughout the year to deepen and update employees on company safety procedures. Special training on the safety of prototypes is given to the prototyping staff, while new staff who have not yet received this training are given training before starting on confidential projects.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up



8.2.4 To what extent are security classifications of the project and the resulting security measures known?

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Each prototyping project is classified as confidential, the classification criteria and the security measures to be adopted are present in the IT security Regulation, which each employee receives upon hiring, the content of which is part of the periodic training to which every employee must submit.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
<p>Based on the observations, no deviation was found.</p>
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.2.5 To what extent is a process defined for granting access to security areas?**

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>The procedure for granting authorizations for access to the prototyping areas is activated and controlled and involves an official access request drawn up by the manager and authorized by of the end of the activities related to the authorization</p> <p>Any occasional external staff can enter the protected area only if accompanied by authorized personnel and upon request and authorization. If the external staff carries out continuous or semi-continuous activities they are provided with a badge and access authorization.</p> <p>All external staff must sign an NDA document.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8.2.6 To what extent are regulations for image recording and handling of created image material existent?

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>it is forbidden to use photographic or video capture devices outside the scope of the project. Images and videos are saved in protected areas and are classified as confidential and subject to the relevant procedures for storage, protection and transfer.</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8.2.7 To what extent is a process for carrying along and using mobile video and photography devices in(to) defined security areas established?

Detailed Description (Including Assessment Procedure)
AL3: Considered documents/evidences/audit trail: Guidelines defined for using mobile phones in prototypes protection areas. Prohibition signals are present inside the production departments and technical offices. The following evidences were provided: <ul style="list-style-type: none"><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

### 8.3 Handling of vehicles, components and parts

#### 8.3.1 To what extent are transports of vehicles, components or parts classified as requiring protection arranged according to the customer requirements?

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Unless otherwise established by the customer, Vimercati adopts a procedure for the safe transfer of prototypes, which includes: Masking or safe packaging, authorization for transport outside protected areas, transport traceability and transport register. Vimercati undertakes to respect the customer's safety requirements if they are higher than the standards used</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.3.2 To what extent is it ensured that vehicles, components and parts classified as requiring protection are parked/stored in accordance with customer requirements?**

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Unless otherwise established by the customer, Vimercati adopts a procedure for the safe storage of prototypes, which includes masking or safe packaging, supervision and control when the material is outside protected areas, it is specified that the prototypes are stored outside the areas protected only for the time necessary for transport and viewing/verification by customers. Vimercati undertakes to respect the customer's safety requirements if they are higher than the standards used</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Information Security Rules, July/2024</li><li>• Procedure P208 Access to protected areas, July/2024</li><li>• Procedure P209 Prototype security, July/2024</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8.4 Requirements for trial vehicles

8.4.1 To what extent are the predefined camouflage regulations implemented by the project members?

Detailed Description (Including Assessment Procedure)
AL3: Considered documents/evidences/audit trail: Not applicable due to Company business.
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**8.4.2 To what extent are measures for protecting approved test and trial grounds observed/implemented?**

Detailed Description (Including Assessment Procedure)
AL3: Considered documents/evidences/audit trail: Not applicable due to Company business.
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up



8.4.3 To what extent are protective measures for approved test and trial drives in public observed/implemented?

Detailed Description (Including Assessment Procedure)
AL3: Considered documents/evidences/audit trail: Not applicable due to Company business.
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

## 8.5 Requirements for events and shootings

### 8.5.1 To what extent are security requirements for presentations and events involving vehicles, components or parts classified as requiring protection known?

Detailed Description (Including Assessment Procedure)
AL3: Considered documents/evidences/audit trail: Not applicable due to Company business.
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

8.5.2 To what extent are the protective measures for film and photo shootings involving vehicles, components or parts classified as requiring protection known?

Detailed Description (Including Assessment Procedure)
AL3: Considered documents/evidences/audit trail: Not applicable due to Company business.
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

## 9 Data protection

### 9.1 To what extent is the implementation of data protection organized?

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>General Manager appointed as responsible of data protection (DPO)</p> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Organizational model, Dec/2023</li><li>• Code_Of_Ethics, Dec/2022</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

## 9.2 To what extent are organizational measures taken in order to ensure that personally identifiable data is processed in conformance with legislation?

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Legal office supported to define and review the Organizational Model and the Supervisory Board verify the correct application of these directives.</p> <p>Creation of specific documentation of data protection principles spread throughout the company through the Quality Document System</p> <ul style="list-style-type: none"> <li>• Organization of work groups within the company ready to address all issues relevant to data protection.</li> <li>• Participation of the data protection officer in any matter relevant to data protection.</li> <li>• Documentation of work processes relating to the processing of data for personal identification.</li> <li>• Documentation of the actions of the data protection officer with regard to the assessments of the data protection law.</li> <li>• Confidentiality obligation of employees and subcontractors.</li> <li>• Implementation of technical and organizational measures by the Information Technology Function to support the internal DPO.</li> <li>• Implementation of reporting processes to immediately notify the customer in the event of a data protection incident.</li> <li>• Documentation of subcontracting relationships, including the contractual regulations with the related subcontractors, regarding data protection.</li> <li>• Ability to implement, when necessary, data deletion actions.</li> </ul> <p>The following evidences were provided:</p> <ul style="list-style-type: none"> <li>• Organizational model, Dec/2023</li> <li>• Code_Of_Ethics, Dec/2022</li> </ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**9.3 To what extent is it ensured that the internal processes or workflows are carried out according to the currently valid data protection regulations and that these are regularly subjected to a quality check?**

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Organizational Model includes all these requirements</p> <p>It is ensured that the internal processes or workflows are carried out according to the currently valid data protection regulations through:</p> <ul style="list-style-type: none"><li>• Periodic checks (reviews and internal audits) and optimizations of the data protection management system through integration with the IT infrastructures intended for the purpose.</li><li>• Policies and procedures to maintain confidentiality and integrity during the transfer of personally identifiable data.</li><li>• Policies and procedures and logical and physical control systems to reduce unauthorized access to personal identification data.</li><li>• Compulsory training of employees in charge of processing the customer's personal data.</li><li>• Periodic checks on compliance with the data protection specifications contained within the contracts and customer provisions.</li></ul> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Organizational model, Dec/2023</li><li>• Code_Of_Ethics, Dec/2022</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

**9.4 To what extent are the relevant processing procedures documented with regard to their admissibility according to data protection law?**

Detailed Description (Including Assessment Procedure)
<p>AL3: Considered documents/evidences/audit trail:</p> <p>Organizational Model includes all these requirements</p> <p>Regarding their admissibility under the Data Protection Act, the processing procedures are documented through:</p> <ul style="list-style-type: none"><li>• Tracking of activities relating to the processing of personal identification data documented in accordance with legal requirements.</li><li>• Supporting clients in conducting data protection impact assessments and documenting the results obtained.</li><li>• Immediate information to the customer, where applicable, in the event of illicit data processing in compliance with the various national laws.</li></ul> <p>The following evidences were provided:</p> <ul style="list-style-type: none"><li>• Organizational model, Dec/2023</li><li>• Code_Of_Ethics, Dec/2022</li></ul>
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up