TISAX® Assessment Report from 02 February 2021

Initial Assessment

FIDIA AUTOMOTIVE ENGINEERING SYSTEMS SRL

SX621V

AV20AB

02 February 2021

Version 5.0.1.

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 VDA 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

TISAX® Scope-ID	SX621V
Scope Type	☒ Standard Scope 1.0 *The assessment was conducted according to the TISAX Standard Scope 1.0. The standard scope comprises all processes and involved resources at the sites defi-ned below that are subject to security requirements from partners in the automotive industry. Involved processes and resources include collection of information, storage of information and processing of information.* ☐ Extended Scope *(Add Custom Scope Description if applicable – remove example if not applicable)* *Example: The assessment was conducted according to an TISAX Standard Scope extended to processes and involved resources at the defined sites that are subject to security requirements of partners in the aerospace and defence industry* ☐ Narrowed Scope *(Add Custom Scope Description if applicable – remove example if not applicable)* *Example: The scope of the assessment were only processes and involved resources at the defined sites that are subject to information related to project <xxx> with partner <yyy>.*
Assessment Objectives	☒ Handling of Information with High Protection Level ☐ Handling of Information with Very High Protection Level ☐ Handling of Prototype Components and Parts ☐ Handling of Prototype Vehicles ☐ Use of Test Vehicles ☐ Events and Photo Shootings with Objects in Need of Protection ☐ Handling of Personal Data according to article 28 GDPR ("processor") ☐ Handling with Special Categories of Personal Data (article 9 GDPR) according to article 28 GDPR ("processor")
Assessment Requirements	ACAR – TISAX Specification of Assessment Version 2.0: Family-ID: ISA, Version 5.0

A.2 Verified Locations

Company Name	Address	Location-ID	Contact Person
FIDIA Automotive Engineering Systems s.r.l.	Via Margherita Viganò De Vizzi 93/95 - 20092 Cinisello Balsamo Milano - Italy	L54KR1	Francesco Alessandrino francesco.alessandrino@fidiasystems.com

A.2.1 Initial Assessment

TISAX® Assessment-ID	AV20AB
Assessment Level	AL2
Assessment Method	☒ Plausibility check of self-assessment using evidences and documentation ☒ Interviews with persons involved in the processes of the auditee ☐ On-site Inspection
Assessment Period	<21/01/20213 (Kick-Off Meeting) – 02/02/2021(Closing Meeting)>
Effective Date (Date of Closing Meeting)	<02/02/2021>
Consent of Auditee	The auditee ☐ unqualifiedly agrees on the documented conclusions. ☒ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

Authors

Auditor
Maurizio Genna
Quality Assurance
Bureau Veritas Italia SpA

Torino, 22-12-2020

Francesco Alessandrino - FIDIA Automotive Engineering Systems Srl   Maurizio Genna -Bureu Veritas Italia SpA

Signature

Reviewed

Init..........

MGenna

B. Summarized Results

B.1 Initial Assessment

AL2: Based on the observations during the initial assessment the overall assessment of the scope is:

☒ Conform

☐ Minor non-conform until <date> (if no corrective action is taken, the result will automatically change to major non-conform)

☐ 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”

  ☐ If a suitable corrective action plan is submitted, the status changes to "Minor Non-conform".

In total, {ha} major and {na} minor non-conformities to the assessed catalogues were identified. {ha} of the major non-conformities become minor if suitable measures are determined.

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

Scope Extension Assessment: The overall degree of maturity results from the maturity levels of the company group's location, which has already been fully evaluated (assessment A---), and the maturity levels of the controls selected for each location (see Part E).

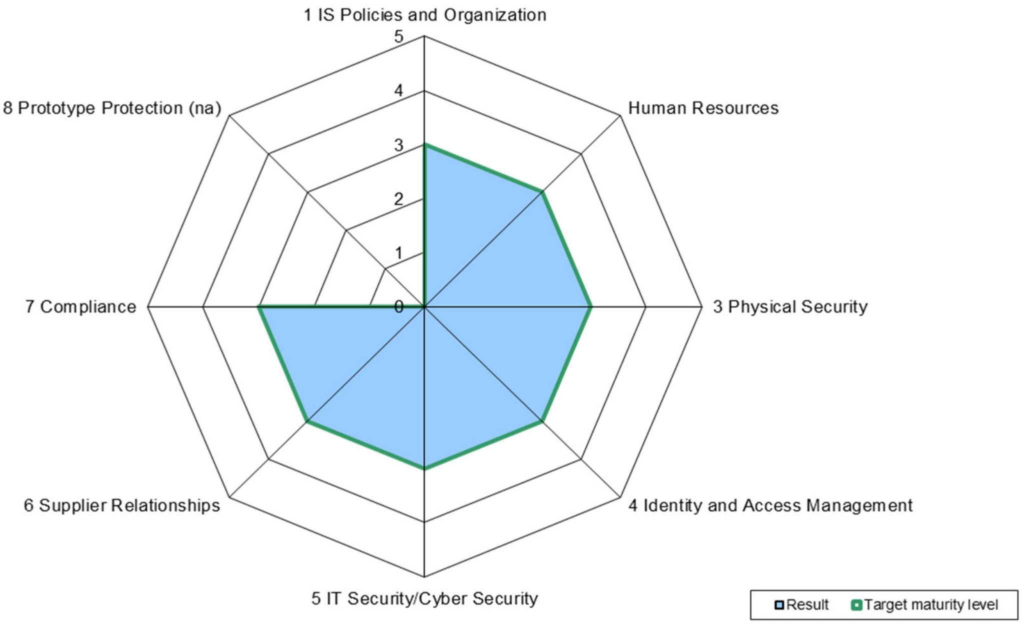
AL2 termination after plausibility check: Based on the results of the plausibility check the description of the implementation in relation to the evidences provided is plausible regarding a large number of requirements. A continuation of the assessment is not effective. The procedure was concluded without result

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.

Result with cutback to target maturity level:	3,00	**Maximum score:**	**3,00**



The following major and minor non-conformities result for the several areas:

No.	Area	Number of major non-conformities[1]	Number of minor non-conformities
1	IS Policies and Organization	0	0
2	Human Ressources	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

Maturity Levels of ISA (Result Tab)

[1] Non-conformities that become major non-conformities solely due to the absence of measures are counted as minor non-conformities in this table.

C.5 ISMS

Based on the current status of implementation, the following maturity levels result for the several controls from chapter ISMS:

No.	Topic	Target maturity level	Result
1	***IS Policies and Organization***		
1.1	***Information Security Policies***		
1.1.1	To what extent are information security policies available?	3	**3**
1.2	***Organization of Information Security***		
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3	***Asset Management***		
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
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	N.A.
1.4	***IS Risk Management***		
1.4.1	To what extent are information security risks managed?	3	3
1.5	***Assessments***		
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6	***Incident Management***		
1.6.1	To what extent are information security events processed?	3	3
2	***Human Resources***		

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

5.2.2	To what extent are development and testing environments separated from operational environments?	3	N.A.
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	***System acquisitions, requirement management and development***		
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	***Supplier Relationships***		
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	***Compliance***		
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

C.6 Handling of Prototypes

The module has not been checked.

D. 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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Isms Manual Issue 0 as of 18/02/2020 and Information Security Policy Rev.0 as of 18/02/2020 inside this Manual; the ISMS Policy distributed and published posted on Company notice boards. The following evidences were provided: → Isms Manual Issue 0 as of 18/02/2020
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Scope. Verified scope in the Tisax excerpt del 04/08/2020 Information Security AL2 # 1 site– Isms Manual Issue 0 as of 18/02/2020– ISMS Responsible nomination (Francesco Alessandrino). and Information Security Policy Rev.0 as of 18/02/2020. FIDIA deals with the design and implementation of works related, initially, to industrial painting systems in the automotive sector; industrial patent consultancy. Management review as of 30/06/2020 (, resources evaluation, suppliers, KPI evaluation, improvement plan-risk analisys-Policy validation, collection of quarterly analisys) ; KPI-indicator table 2020 with December’s analisys (Confidentiality - back up-restart test-HR management-incident-quality back up-malware-NDA-training-virus attack-intrusion, patch management); internal audit (findings insert in VDA check list and active improvement); document “Quarterly Information Security Check” (user-back up-patch-incident-training) done by external supplier (ADS external) as technical check on technical infrastructure (none NC or anomalies).

The following evidences were provided:

- Tisax Excerpt SF6HLC 28/07/2020
- Isms Manual Issue 0 as of 18/02/2020
- Asset detail report dated 20/01/2021 done by Nathan Srl

Finding

Based on the observations, no deviation was found. (da rvedere il riesame della direzione)

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Nominative organization chart App. A MSGSI rev.0 del. 18/02/2; letter of appointment as IT administrators (#4) and treatment data for external ICT manager and internal ISMS manager (granted separation of duties); checked also internal NDA signed by employees. The following evidences were provided: The following evidences were provided: • Organizational chart as of 01 October 2020
Finding
Based on the observations, no deviation was found.
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Procedure PG05 Operational activities - design with indication of project classification (public confidential) as of 04/10/2019 (9001 procedure)-Risk analysis in projects –; risk assessment for each project; if any faults on aspects of information sec are foreseen in the case of high protection need. Additional risks are analyzed during the opening phase. Three levels of information's classification (confidential, controlled and public) as specified in ISMS Manual Par. 7.5.4.

The following evidences were provided:

- planning design; project start report filled in;
- ISMS Operating Manual MSGSI rev. 0 of 18/02/20, par. 8.1 2
- OPERATIONAL PLANNING AND CONTROL "PG05 Operational activities - design.
- Project and Development Plan 05_01 / pps
- Design Review Report 05_01 / rv

Finding

Based on the observations, no deviation was found.

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: **Cloud: the organization does not use externally provided IT services, which is not applicable**
Finding
Based on the observations, no deviation was found.
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Asset inventory-asset management. An inventory of critical information assets exists (Mod. 03 – ELA). Reduced list because the company does not have many technological infrastructures (server-PC)

- Each critical information asset is assigned the respective supporting assets.

- The inventory is reviewed at regular intervals.

The Risk Assessment done is based on Asset Management (Mod. 07 PSAI)

The following evidences were provided:

- ISMS Operating Manual MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL ",
- Risk Management PG 02 rev. 1 of 18/02/20,
- procedure" Use of IT tools "PG 09 rev. 0 of 18/02/2020

Finding

Based on the observations, no deviation was found.

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Information classification : three levels of information's classification (confidential, controlled and public) as specified in ISMS Manual Par. 7.5.4.All documents inside the folders take the classification of the same. The following evidences were provided: • ISMS Operating Manual MSGSI rev. 0 of 18/02/20
Finding
Based on the observations, no deviation was found.
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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: **Cloud services.** **Cloud: the organization does not use externally provided IT services, the point is not applicable**
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Context and risk analisys PG02 as of 01/09/2020 .Risk assessment report as of 18 December 2020 with results with weekness in the following sector with related treatment plan inside the report; focus on obsolescence of physical and logical infrastructures and on external risks. The risk analysis has also been extended to business processes (commercial-purchasing).
Operational continuity plan IST 02 rev. 0 of 18/02/2020: natural events-pandemic with last report of simulation dated
Pandemic management: each manager has his own office, so it was possible to all stay in the office (4 people per 200 square meters); manage activities with customers remotely. Under the reception there is a temperature scanner that blocks people and prevents them from proceeding in the offices.
Laptops: evaluate the possibility of having a portable forklift in case of failure of one of those used
UPS: 30 minutes (estimated that there have been no interruptions of more than 5 minutes in the past);
Connectivity: Vodafone + sim back up 4g in case of data loss.
The following evidences were provided:

- Risk assessment report as of 30 June 2020
- Context and risk analisys PG02 as of 01/09/2020
- Operating Manual of the SGSI MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL

Finding

Based on the observations, no deviation was found.

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 9.1 "MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION". Bimonthly verification of security done by external IT Supplier (Nathan Srl)

Latest bimonthly report from Nathan on IT infrastructures with the following contents:

1. 3 machines + 1 machines (4 laptops -1 physical server)

2. PC machine status (4) -Server - NAS

3. Patch management

4. Hardware life cycle

Internal audit done by external Consultant on 29 June 2020 with related plan.Audit done every year.

The following evidences were provided:

- Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 9.1 "MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION"
- Bimontly report by Nathan Srl
- Internal Audit report
- Form 06 / go Internal audit report, Form 07 / PSAI
- Surveillance and action plan
- Form 07 / vrd Management Review Report

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 9.1 "MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION"; Internal audit done by external Consultant on 20/06/2020. Independence is guaranteed by the check made by the IT Manager and Management. The following evidences were provided: • Internal audit done by external Consultant on 20/06/2020 on VDA 5.1 requirements • Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 9.1 "MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION"
Finding
Based on the observations, no deviation was found.
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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Instruction "Reporting and managing incidents" IST-03 rev. 0 of. 16/01/2020, 'Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL The following evidences were provided: None incident issued
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Operative Manual del SGSI MSGSI rev. 0 del 18/02/20, par. 7. : Disciplinary process (Company regulation) - code of conduct - agreement with each worker - confidentiality agreements drawn up by employees. Checked confidentiality agreements drawn up by employees signed by employees valid until Law revision. Critical figures: designers, process and electrical Engineering.

Checked: competences analisys and profiles; training report as of 02 march 2020 related ISO 27001 requirements; training plan.

The legal requirements are taken into consideration both in terms of Collective Labor Agreement and Privacy

The following evidences were provided:

- Operative Manual del SGSI MSGSI rev. 0 del 18/02/20, par. 7
- Records related competences and training (personnel files)

Finding

Based on the observations, we raccomended to the Organization to. **Better plan awareness training/information actions finalized to prevent potential incident (the organization is currently small and made up of worker administrators)**

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Operative Manual del SGSI MSGSI rev. 0 del 18/02/20, par. 7; Ethic Code MG001 Ce with sanctions regime - agreement with each worker - confidentiality agreements drawn up by employees.

The following evidences were provided:

- Checked samples of confidentiality agreements drawn up by employees signed by employees valid until Law revision
- Corporate regulation paragraph §Commitment to confidentiality
- Ethic Code MG001 Ce

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Training plan 2020 with courses in December about informations security and informations management, incident management, GDPR, ISMS documentation and checked training document (all 2020 training course done and records are available);
Information – awareness: training and information about social engineering technics and phishing; Operative Manual del SGSI MSGSI rev. 0 del 18/02/20, par. 7; Internal Training Course Planning awareness e training – training done in 2020 .Training done in Production and Design dpt.

The following evidences were provided:

- checked training report and effectiveness control during audit § Smart Working Rules (done on 02 March 2020)
- checked training minutes and list of participants
- There are specific KPI about training (% completion on personnel – total employees); trimestral check on training activities (planned – done)

Finding

Based on the observations, no deviation was found. (see point 2.1.1.)

Planned measures (including implementation period)

Evaluation at Follow-Up

2.1.4 To what extent is teleworking regulated?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

The organization has defined and treated smart working during the Covid period and will use this working methodology also in the future. Teleworking, as defined by the Italian legislation, is not contractually treated.

The following evidences were provided:

- Company regulation (ref. 1.1.1)
- § Smart Working Rules
- §Portable PC use

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Rules/Procedures for access to the headquarters; Directional Building:FIdia offices are loicated at 7^ floor;-guardian site is active to filters attendance-accompaniment in offices.

No storage area only offices (alarm on each floor) - seen the access control document of the Building Property delta which defined the access rules;

Office photo views with indication of the access points monitored by CCTV-alarm-badge systems. Server room view with mini rack (server-NAS-ups-switch) For key server room.The following evidences were provided.:

- Regulations for access to the company
- ISMS description paragraph § Physical perimeter; § Physical Security Measures
- Floorplan-FIdia
- Pictures Windows with films
- Photo anti-theft sensor
- Photo Video Surveillance access main entrance

Finding

Based on the observations, no deviation was found.

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Business continuity plan IST-02 rev. 0 of 13/01/2020. 'Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL. Risk Management Procedure PG 02 rev.1 of 18/02/20:

Back up: back up rules on NAS via Synology sw daily at 3 am and back up file server 22. In case of fail or data loss messages arrive to ads. Back up situation view updated to today (only one problem on 12/01 (then manually redone). Only for servers and not laptops as everything is saved on file server. FIdia is supported by external IT supplier (Nathan Srl) that could help India in emergency / incident events.Pandemic management : in a week they managed the situation to make everyone operational from home, activating the VPNs. Checked Open VPN tool to monitor download/upload; VPN encrypted with certificate installed on PCs.

The following evidences were provided:

- ISMS description paragraph § Organizational Measures (Redundancy) ref. 1.2.1
- Business Continuity Plan
- Technical Specifications HW Configuration
- BCP simulation dated 14 December 2020 (Flooding emergency simulation and power failure)

Finding

Based on the observations,It’s been recommended to the Organization to. **About the failure back up messages must be informed also Fidia (by mail or SMS), not only Nathan Srl (in any case Nathan informs Fidia of all problems in the periodic report).**

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

ISMS Description § Organizational Security Measures; Requirement specifications are subject to quarterly review during ADS audits for compliance with defined policies and changes in the environment. Each new IT system is evaluated according to the policies defined before implementation. In the event of significant changes to the IT infrastructure, a Vulnerability Assessment is assessed

The following evidences were provided:

- Company regulation (ref, 1.1.1)
- §Using portable PCs
- §Dismission of IT Devices (drilling hard disk)
- ISMS description paragraph § Organizational Security Measures (ref. 1.2.1)

Finding

Based on the observations,It’s been recommended to the Organization to. **provide for a spare PC configured for operational continuity in the event of a PC breakdown**

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Company Guide Lines Information Security as of July 2020 Removable media-encryption of media : In FIdia it is not allowed to use mobile devices to store information. In FIdia it is allowed to use encrypted mobile devices for transfer of information in case of problems of use with the client platforms in use. USB and external HD are prohibited. Management may have encrypted USBs available. Dismission of IT Devices-ISMS description paragraph § Organizational Security Measures (ref. 1.1)- To guarantee the confidentiality of the data, to avoid the risk of unauthorized access to the data stored on the media sent for disposal, each support, depending on whether it is intended for re-use or final disposal, is treated as follows: • Reuse within FIdia S.r.l .: low-level formatting • Final disposal: physical destruction (drilled with HD drill) The following evidences were provided: • Checked samples of USB port locked and controlled/scanned of threats by Sengfor Endpoint Secure
Finding
Based on the observations, no deviation was found.
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Policy User management_rev.00 as of 01/10/2020. Some user opening card forms were checked on a random basis with details on privileges, printers; Fidia has few IT infrastructures, mainly laptop and servers. Is available a network map updated 2020.

The following evidences were provided:

- Checked table with read / write access rights to system folders.
- ISMS description paragraph § Logical Security Measures
- Company regulations §Use of authentication devices (Badges, etc.)
- Asset detail report dated 20/01/2021 done by Nathan Srl
- FIDIA_Mod. 03-ELA Equipment List

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Confidentiality: FP033 GE&PM; all IT administrators can access the folders, but technicians cannot access the financial / contractual and procurement parts. In the design review (project by project) it is defined who will work on the job, using macro areas with access passwords. Matrix view with access properties on folders. Users who have access to folders including patents have signed NDA.

Users: requested to Nathan opening users via email; no temporary users and no opening / closing users in the last 6 months.

The following evidences were provided:

- PG_009_ Using Enterprise IT Tools and Services,
- 'OPERATIONAL MANUAL OF THE SGSI MSGSI rev. 0 of 18/02/20,par. 8.1 2PLANNING AND OPERATIONAL CONTROL

Finding

Based on the observations, no deviation was found.

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Confidentiality: FP033 GE&PM; all administrators can access the folders, but technicians cannot access the financial / contractual and procurement parts. In the design review (project by project) it is defined who will work on the job, using macro areas with access passwords. Matrix view with access properties on folders. Users who have access to folders including patents have signed NDA.

- 'PG_009_ Using Enterprise IT Tools and Services

Finding

Based on the observations, no deviation was found.

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?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

'PG_009_ Using Enterprise IT Tools and Services - Company regulation paragraph § Password management par. 8.1 2PLANNING AND OPERATIONAL CONTROL. . Server with hierarchical tree with active directory groups; in the projects folder, the subfolders (for customers) broken folder inheritance, removed security locks.

Confidentiality: FP033 GE&PM; all administrators can access the folders, but technicians cannot access the financial / contractual and procurement parts. In the design review (project by project) it is defined who will work on the job, using macro areas with access passwords. Matrix view with access properties on folders. Users who have access to folders including patents have signed NDA.

The Chinese shareholder does not have access to the System, the sharing takes place with SFTP; transmission of documents depends on the customer:

1.Structured customers (VW type) has a site where it deposits the documents and you can download documentation upon approval as a supplier; or upload the documentation;

2.Other customers use site for heavy documentation; for the lighter one, e-mail is used without any particular encryption methods.

The following evidences were provided:

- 'PG_009_ Using Enterprise IT Tools and Services.
- 'Operational Manual of the SGSI MSGSI rev. 0 of 18/02/20,
- par. 8.1 2PLANNING AND OPERATIONAL CONTROL

Finding

Based on the observations, no deviation was found.

Planned measures (including implementation period)

Evaluation at Follow-Up

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Cloud transfer for SFTP manual paragraph § Data encryption; tool Bitlocker; par. 8.1 2PLANNING AND OPERATIONAL CONTROLBitlocker HDEncryption; According to the Project Classification Policy, as well as legal and contractual obligations The following evidences were provided: • PG_009_ Using Enterprise IT Tools and Services. • 'Operational Manual of the SGSI MSGSI rev. 0 of 18/02/20, • par. 8.1 2PLANNING AND OPERATIONAL CONTROL Bitlocker HD Encryption • Checked a sample of HD cryptography with screenshot of the steps
Finding
Based on the observations, no deviation was found.
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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: PG_009_ Using Enterprise IT Tools and Services. Operating Manual of the SGSI MSGSI rev. 0 of 18/02/20, par. 8.1 2PLANNING AND OPERATIONAL CONTROL. INFORMATION SECURITY POLICY" rev.0 of 18/02/2020- the exchange of data / documents with the customer is carried out with the FTP platform ; access to customer portals is managed by SSL certificates and secure connections (Clients' Responsibility). The following evidences were provided: • PG_009_ Using Enterprise IT Tools and Services. Operating Manual of the SGSI MSGSI rev. 0 of 18/02/20, par. 8.1 2PLANNING AND OPERATIONAL CONTROL. INFORMATION SECURITY POLICY" rev.0 of 18/02/2020 • File exchange is provided through SFTP areas.
Finding
Based on the observations, no deviation was found.
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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: There are no particular changes from a structural point of view. For the changes, improvement plans provided for by 9001 are used. The following evidences were provided: • Operational Manual of the SGSI MSGSI rev. 0 of 18/02/20, • par. 8.1 2PLANNING AND OPERATIONAL CONTROL, • par. 9.1 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION
Finding
Based on the observations, no deviation was found.
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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: **Not applicable - No software developed** The following evidences were provided:
Finding
Based on the observations, no deviation was found.
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Check for Windows updates every Wednesday every lunch break.

All systems and applications are patched; antispam and antivirus on firewalls.

Monitoring system with technology used by DattoRMM; patched all network devices except the printer.

Website is on Kaliweb; file server on Microsoft server. The only open vs external port is https for remote VPN and firewall management.

Antivirus: webroute updated every day.The following evidences were provided:

- Manuale Operativo del SGSI MSGSI rev. 0 del 18/02/20,
- par. 8.1 2PIANIFICAZIONE E CONTROLLO OPERATIVIScreenshot Antivirus management panel
- Checked, on Client control panel, the daily update and blocking of some potential threats

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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

FIdia manages Logs (security Logs-instrusion detection-access Logs-admin Logs), all encrypted. The retention is set to always. System administrator logs are all encrypted tool

The following evidences were provided:

- 'Operational Manual of the SGSI MSGSI rev. 0 of 18/02/20,
- par. 8.1 2PLANNING AND OPERATIONAL CONTROL

Finding

Based on the observations, no deviation was found.

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: 'Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL. Risk Management Procedure PG 02 rev.1 of 18/02/20 access regulation. Windows updates are not automatically installed by the automatic Windows Update procedure on both the servers and the client, are manually checked and installed after a security evaluation. - Adequate license, update and patch management for customer platform software. - Adequate patch management - Check for Windows updates every Wednesday every lunch break. --All systems and applications are patched; antispam and antivirus on firewalls. --Monitoring system with technology used by DattoRMM; patched all network devices except the printer. The following evidences were provided: • Users behavior Report done by Nathan Srl dated 29/01/2021 • Outbound Security Report done by Nathan Srl dated 29/01/2021 Description
Finding
Based on the observations, no deviation was found.
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Remote Monitoring & Vulnerability Management .Technical controls on IT infrastructures are done with internal system monitoring (Bimonthly done by Nathan Srl). Every year is done a VA assessment with NET Anathomy tool with report as output. Website is on Kaliweb; file server on Microsoft server. The only open “door” vs external port is https for remote VPN and firewall management, so the PT is been evaluated unnecessary. .

The following evidences were provided:

- • Windows patch report done by Nathan dated 29/01/2021
- Reports VA 2019-2020-2021

Finding

Based on the observations, no deviation was found.

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: ISMS description § Logical Security Measures Company regulations paragraph § Network use Risk Analysis. Extended requirements for the control and management of networks are determined and implemented. #2 lines Vodafone. The following evidences were provided: • Checked, with video, server room (server+NAS, air system, firefighting system).
Finding
Based on the observations,It's been recommended to the Organization to **:** **Provide server temperature probe to monitor the temperature (no security issues).** **Provide physical key management log for accessing the server room (no security issues).**
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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: ISMS Description § Organizational Security Measures; Requirement specifications are subject to quarterly review during ADS audits for compliance with defined policies and changes in the environment. Each new IT system is evaluated according to the policies defined before implementation. In the event of significant changes to the IT infrastructure, a Vulnerability Assessment is assessed The following evidences were provided: • ISMS Description § Organizational Security Measures
Finding
Based on the observations, no deviation was found.
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

A segmentation of the FIdia network is implemented through the management of permissions for the different user groups by ADS and Resp ISMS; Network structure: two virtual machines, network and external. Switch provide segmentation even if redundant (switch back up of the other). Senford tool aim IT manager to test for segmentations, connections, latency and any packet loss

The following evidences were provided:

- SLA monitoring of connectivity providers - Agreement for the provision of Spazio Web (Cloud-Internet Services)
- PGMG01-Incident Safety Management Procedure
- ISMS description paragraph § Organizational Security Measures

Finding

Based on the observations, no deviation was found.

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: A procedure for returning and securely removing information assets from any external IT service is defined and implemented.; Fidia doesn’t use Cloud Services.. The following evidences were provided: • Operational Manual of the SGSI MSGSI rev. 0 of 18/02/20, • par. 8.1 2 OPERATIONAL PLANNING AND CONTROL, • par. 9.2 INTERNAL AUDITS . "REGULATION OF USE OF IT TOOLS" Information security policy
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?

Detailed Description (Including Assessment Procedure)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: hw and sw assistance and maintenance is entrusted to an external company (Nathan) for which we have seen NDA (signed as system administrator) and the data processing management letter The following evidences were provided: • ISMS description paragraph § Logical Security Measures ref. 1.2.1 • Risk Analysis • NDA – personal data treatment with Nathan
Finding
Based on the observations, no deviation was found.
Planned measures (including implementation period)
Evaluation at Follow-Up

6 Supplier Relationships

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

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

'Procurement Procedure ISO 9001- Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL; NDA; a list of critical supplier is available (#20 – Nathan srl-Proget)); none non conformities (neither at the infrastructural level nor document loss.

Two types of NDA: internal and for suppliers.

NDA visa signed by Acorncapital for tax relief for the development of a project (patent) on 27/7/2020.

NDA visa to LSPE (engineering company) signed on 29/01/2021.

The following evidences were provided:

- 'Procurement Procedure PO 04 rev.1 of 18/02/20.
- Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROLPGAC01_5 Monitoring of suppliers
- Suppliers' NDA
- Supplier evaluation updated 2020

Finding

Based on the observations, no deviation was found.

Planned measures (including implementation period)

Evaluation at Follow-Up

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

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

'Procurement Procedure. Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROL

The following evidences were provided:

Description

- 'Procurement Procedure PO 04 rev.1 of 18/02/20.
- Operational Manual of the ISMS MSGSI rev. 0 of 18/02/20, par. 8.1 2 OPERATIONAL PLANNING AND CONTROLPGAC01_5 Monitoring of suppliers
- Suppliers' NDA
- Supplier evaluation updated 2020

Finding

Based on the observations, no deviation was found.

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)
AL2: The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation: Applicable Regulations List -Asset Inventory with License Management. A list of Laws applicable in FIdia is available and updated (updated September 2020). GDPR documentation is present (information, treatment register). The customer's specifications are archived as binding contractual documents. The following evidences were provided: • Applicable Regulations List • Customer Specifications List • License Management • Company regulation
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)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

GDPR manual is present. Contracts and compliance. Aspects of confidentiality, security and privacy are applied in the Company.

The following evidences were provided:

- Checked # 2 samples of Treatment Data Letter signed by Fidia and Employee.
- Checked # 2 samples of Treatment Data Letter signed by Fidia and Suppliers
- GDPR Documentation

Finding

Based on the observations, no deviation was found.

Planned measures (including implementation period)

Evaluation at Follow-Up