TISAX® Assessment Report

Initial Assessment

Triangl, a.s.

SCHWYY

AV65AM

21.11.2023

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 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	SCHWYY
Scope Type	☒ Standard Scope 2.0 *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.* *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.* ☐ Custom Extended Scope ☐ Full Custom Scope
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 2.1: Family-ID: ISA, Version 5.0

A.2 Assessed Locations

Company Name	Address	Location-ID	Contact Person
Triangl, a.s.	Beranových 65 19902 Praha Czech Republic	L5K715	Věra Továrková vera.tovarkova@trianglprint.cz

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

A.3 Initial Assessment

TISAX® Assessment-ID	AV65AM-1
Assessment Level	AL2
Assessment Method	☒ Plausibility check of self-assessment using evidence and documentation ☒ Detailed evaluation of evidence ☒ Interviews with persons involved in the processes of the auditee ☐ On-site Inspection ☐ Video based remote site inspection
Date of Kick-Off Meeting	03.11.2023
Date of Opening Meeting	20.11.2023
Date of Closing Meeting (Effective Date)	21.11.2023
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
Jaromír Tvrzník
Quality Assurance
Věra Továrková

Praha, 21.11.2023

Signature

Signature

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 (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 (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.

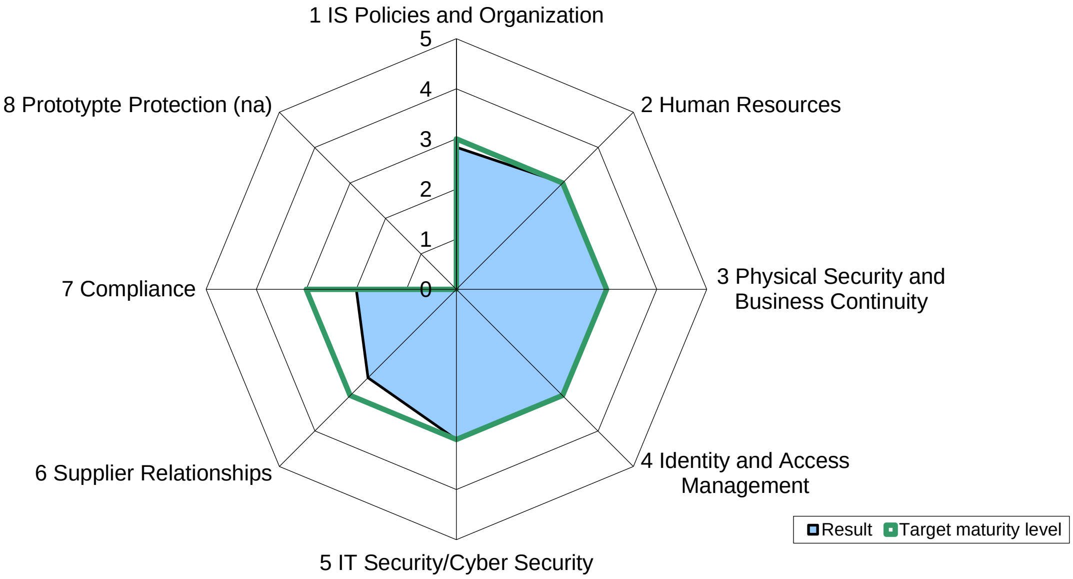
After the initial assessment an average maturity level of 2,89 was calculated.

As no non-conformities identified during this assessment, the auditor **recommends to issue full label in above mentioned scope.**

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	N/A	N/A
9	Data Protection	N/A	N/A

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.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	**2**
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 the responsibilities between external IT service providers and the own organization defined?	3	**3**
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	**3**
1.4.1	To what extent are information security risks managed?	3	**2**
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 authority?	3	**3**
1.6.1	To what extent are information security events processed?	3	**3**
2.1.1	To what extent is the qualification 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**
3.1.1	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**

4.1.1	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**
4.2.1	To what extent are access rights assigned and managed?	3	**3**
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 transfer?	3	**3**
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	**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**
5.3.1	To what extent is information security considered in new or further developed 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**
6.1.1	To what extent is information security ensured among contractors and cooperation partners?	3	**2**
6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	3	**3**
7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?	3	**2**
7.1.2	To what extent is the protection of personally identifiable data taken into account when implementing information security?	3	**2**

D.2 Handling of Prototypes

The module has not been assessed.

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)

AL2:

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

- SM 1-1-4 Příručka ISMS 27001
- ZA 6-1-7 Cíle a programy ISMS
- SM 8-3-1 Standardy informacni bezpecnosti
- SM 4-2 Kontext organizace ISMS
- SM 5-1 Vůdčí role vedení ISMS
- ZA 5-2-1 POLITIKA ISMS
- Jmenovací dekrety ISMS

Description

The following evidence were provided:

The organization has implemented an information security management system. The main document (SM 1-1-4 Příručka ISMS 27001) describes the level and requirements of the implementation of Information security. The requirements for information security are determined and documented (SM 1-1-4 Příručka ISMS 27001 and ISMS 5 SM 8-3-1 Standardy informacni bezpecnosti). The requirements are adapted to the goals of the organization (ZA 6-1-7 Cíle a programy ISMS). The policy has been created in collaboration with an external advisor and approved by the organization's management. In the policy are reflected security requirements based on the strategy of the organization, regulative and contractual obligations. All ISMS goals have an owner and date. Policies are available to employees in a suitable form on OneDrive. Policy are periodical review (1x12 months).

Finding

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

Description: Some ISMS policies were not formally signed.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

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:

- SM 1-1-4 Příručka ISMS 27001
- ZA 6-1-7 Cíle a programy ISMS
- SM 8-3-1 Standardy informacni bezpecnosti
- SM 4-2 Kontext organizace ISMS
- SM 5-1 Vůdčí role vedení ISMS
- ZA 5-2-1 POLITIKA ISMS
- ZA 7-1-3-2 Jmenovací dekrety ISMS
- ZA 6-1-5 Prohlášení o aplikovatelnosti ISMS
- SM 4-3 Výbor kybernetické bezpečnosti
- ZA 9-3-1 Zpráva o přezkoumání_ISMS

Description

The following evidence were provided:

The scope of the ISMS is defined without excluding.
Applicable controls are identified in the Statement of Applicability and KPI controls. The organization's requirements are described in the document Information Security. The organizational management has commissioned and approved the ISMS through the SM 8-3-1 Standardy informacni bezpecnosti, published 1.3.2023. The effectiveness of the ISMS is regularly reviewed by the management through the document ZA 9-3-1 Zpráva o přezkoumání_ISMS.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- MKB, AKB, VKB roles
- Employee training record
- SM 6-1 Plánování ISMS
- SM 7-1-1 Podpora systému ISMS
- SM 8-1 Řízení provozu

Description

The following evidence were provided:

Responsibilities for information security within the organization are defined, documented, and assigned - organization-appointed security roles (MKB, AKB, VKB) and further trained employees. The responsible employees are defined and qualified for their task - for security roles in the document SM 8-3-1 Standardy informacni bezpecnosti, for the employees in the document Desatero pro uživatele and Contact person are known within the organization and to relevant business partners - via email and training.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 20 Standardy informacní bezpecnosti
- List of Projects
- Desatero pro uživatele

Description

The following evidence were provided:

Projects are classified considering their information security requirements in "Founding documents of the project". The list of projects is recorded in an Excel table. The organization has established 3 degrees of information classification. Customer information is always included in the category Internal or Confidential. C - Confidential (based on the customer's request for increased information security) and category I - Internal (without the customer's request for increased information security). The classification of the document is always indicated in the project charter.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 1-1-10 Hodnoceni dodavatelu

Description

The following evidence were provided:

The security requirements are relevant to the IT service are determined and described in the document Standardy informacni bezpecnosti. IT services are provided as an internal onsite service.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 6-1-3 Rizika_ISMS
- ZA 6-1-4 Plan zvladani rizik2022
- ZA 9-1-1 Plán monitorování ISMS
- SM 6-1 Plánování ISMS

Description

The following evidence were provided:

Information assets of critical value to the organization are identified and recorded in the IS Alvao and in document ZA 6-1-3 Rizika_ISMS. A person responsible for these information assets is assigned and recorded in the document ZA 6-1-3 Rizika_ISMS. The supporting assets processing the information assets are identified and recorded in the document ZA 6-1-3 Rizika_ISMS. The inventory is reviewed at regular intervals.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Desatero pro uživatele
- ZA 6-1-3 Rizika_ISMS
- ZA 6-1-4 Plan zvladani rizik2022
- ZA 9-1-1 Plán monitorování ISMS
- SM 6-1 Plánování ISMS

Description

The following evidence were provided:

A consistent scheme for the classification of information assets with regard to the protection objective of confidentiality is available in the document Standardy informacni bezpecnosti and in document Desatero pro uživatele.
Requirements for the handling of supporting assets (e.g., marking, correct handling, transport, storage, return, deletion/disposal) depending on the classification of the information assets exist and are described.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 1-1-10 Hodnoceni dodavatelu

Description

The following evidence were provided:

The organisation has established a process of evaluation of external IT services. External IT services are part of risk assessment (clouds). Purchasing of external IT services must be approved by the General Director. External IT services are regularly reviewed from the view of existing ISMS certification, NDA agreement, and a number of complaints.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 6-1-3 Rizika_ISMS
- ZA 6-1-4 Plan zvladani rizik2022
- ZA 9-1-1 Plán monitorování ISMS
- SM 6-1 Plánování ISMS

Description

The following evidence were provided:

Risk assessments are carried out both at regular intervals (1x12 months) and in response to events (e.g., Critical Security incident). Information security risks are assessed suitably according to the probability of occurrence and potential damage. Information risks are documented, risk owner is assigned to each threat. A procedure to identify, assess, and address information security risks within the organization is in place (ZA 6-1-4 Plan zvladani rizik). Criteria for the assessment and handling of information security risks exist (SM 6-1 Plánování ISMS).

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

Description: Risk analysis exists, but some risks are not formally assessed.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 9-1-1 Plán monitorování ISMS
- ZA 9-2-1 Program interních auditů ISMS
- ZA 9-2-2 Zápis z auditu ISMS
- ZA 10-2-1 Kniha nápravných opatření

Description

The following evidence were provided:

Observation of policies is verified throughout the organization by Internal audits and KPIs. Information security policies and procedures are reviewed at regular intervals (1x12 months). Managers perform random inspections. Nonconformities are reported to VKB. Compliance with information security requirements is verified at regular intervals. The results of the conducted reviews are recorded (ZA 9-2-2 Zápis z auditu ISMS). There is a plan for content and framework conditions (time schedule, scope, controls) of the reviews to be conducted is provided (ZA 10-2-1 Kniha nápravných opatření).

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 9-1-1 Plán monitorování ISMS
- ZA 9-2-1 Program interních auditů ISMS
- ZA 9-2-2 Zápis z auditu ISMS

Description

The following evidence were provided:

Information security reviews are carried out by an independent body (external auditor Mr. Chlup) at regular intervals (1x12 months). Measures for correcting potential deviations exists (ZA Kniha NO).

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Bezpečnostní incidenty v ticketovacím nástroji
- Desatero pro uživatele

Description

The following evidence were provided:

A definition of information security events/vulnerabilities exists - security events and security incidents. A procedure for reporting and recording information security events/vulnerabilities is defined and implemented via email.
Information security incidents are reported via email and Excel table.
vera.tovarkova@trianglprint.cz
+420 606 939 180

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- HR dokumentace
- Nástupní list

Description

The following evidence were provided:

Sensitive work fields and jobs are determined. The requirements for employees with respect to their job profiles are determined and fulfilled. The identity of potential employees is verified (e.g., checking identity documents). All employees have a signed NDA.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- NDA
- Školení a presencní listina
- Vzorová smlouva

Description

The following evidence were provided:

All employees have NDA obligations. A non-disclosure obligation is effective beyond the employment contract - 3 years.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- NDA
- Školení a presencní listina
- Desatero pro uživatele

Description

The following evidence were provided:

A concept for awareness and training of employees is prepared. Main themes:
- Information security policy
- reporting of information incidents
- reaction of malware
- Password policy
- compliance issues of information security
- NDA requirements

The training is for all employees. The concept has been approved by the CEO. Training is carried out at regular intervals (1x12 months). Participation in training and awareness measures is documented.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Desatero pro uživatele

Description

The following evidence were provided:

The requirements for teleworking are determined and fulfilled. The following aspects are considered:
 - secure handling
 - Home Office

Access to the organization’s network is gained via a secure connection VPN.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Zony Triangl
- Provozni řád červené zóny
- SM 21-1 Ochrana prototypu

Description

The following evidence were provided:

A security zone concept including the associated protective measures based on the requirements for handling information assets is defined and documented. In the organization exist 3 zones:
 - white
 - orange
 - red

The code of conduct for security zones is known to all persons affected. Procedures for allocation and revocation of access rights are established - for employees MKB or General director, for visitor’s General director.
Network/infrastructure components are protected against unauthorized access - via password or certificate.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 6-1-3 Rizika_ISMS
- ZA 6-1-4 Plan zvladani rizik2022
- ZA 8-1-1-2 Plán kontinuity
- SM 8-1 Řízení provozu
- Recovery mailové schránky

Description

The following evidence were provided:

Possible exceptional situations are identified and recorded in Risk analysis and emergency plans. Emergency plans are defined and reviewed regularly (1x12 months).
Information security measures for crisis situations are tested regularly results are recorded.
Appropriate protective measures (e.g., fire alarm system, fire protection) are implemented and regularly checked.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Desatero pro uživatele

Description

The following evidence were provided:

The requirements for handling assets are determined. Responsibility for it is the IT Department. For security transport exists USB flash with cryptographic. The overwrite method (0 and 1 over the whole disk) is used for secure deleting. All confidential information is recorded on a secure NAS.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Desatero pro uživatele
- Identifikace aktiv v IS Excel

Description

The following evidence were provided:

The requirements for mobile IT devices and mobile data storage devices are determined and fulfilled. The following aspects are considered:
- access protection - PIN or Password
- BitLocker on notebooks
- registration of IT devices (type and username). Mobile IT devices are recorded on the SW.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- HR dokumentace

Description

The following evidence were provided:

Identification of approaches to individual parts is kept within the HR documentation. Upon termination of employment, the authentication means must be returned to IT immediately and deactivated.
In case of loss of access means, the employee is obliged to report this immediately to the email vera.tovarkova@trianglprint.cz
+420 606 939 180
and enter the security incident in the ticketing tool. MKB, together with the IT department, will deactivate the authentication means so that it cannot be misused.
If it is necessary to change the authorization on the authentication means, the superior requests the change using the ticketing tool.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- kontrola pristupu 2022

Description

The following evidence were provided:

Every user has their name and password, The procedure for users is based on the princip need to know and the least privileges. For standard users, 10 characters, and contains one uppercase letter and a number, for privileged password is valid at 10 characters, full complexity.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- kontrola pristupu 2022

Description

The following evidence were provided:

The creation, modification, and deletion (lifecycle) of user accounts are performed. Via ticketing tool.

Every user has a unique and personalized account.

User accounts are disabled immediately after the user has resigned from or left the organization.

User accounts are regularly reviewed (1x12 months) on AD.

A basic user account template with minimum access rights and functionalities is defined and used.
Default accounts and passwords pre-configured by manufacturers are disabled.
User accounts are created or authorized by the IT department.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- kontrola pristupu 2022

Description

The following evidence were provided:

Access rights management is controlled by a manual protocol. All accounts are created on need-to-know principles.

Access rights are reviewed at regular intervals (1x12 months)

Normal user accounts are not granted privileged access rights.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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: • SM 8-3-1 Standardy informacni bezpecnosti Description The following evidence were provided: Cryptographic procedures for HTTPS, VPN, and SSL are identified.
Finding
Based on the observations, no deviation was found. AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.
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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Desatero pro uživatele

Description

The following evidence were provided:

Information type C - confidential must be during transport encrypted.
A list of networks exists and is stored on the internal wiki. The organisation has 3 networks. One for employees, one for WIFI for employees, and a third for guests.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Ticketing system
- Desatero pro uživatele

Description

The following evidence were provided:

Changes for critical assets are recorded in the ticketing system.
A formal approval procedure is established and done through the ticketing system. Changes are checked and evaluated for potential impacts on information security through testing before implementation on release.
Changes affecting information security are planned and tested.
Procedures for fall-back in fault cases are taken into account.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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: • SM 8-3-1 Standardy informacni bezpecnosti Description The following evidence were provided: Test, development, and operational systems are separated from each other in such a way that they cannot be negatively influenced by each other. I.e., are operated on other servers separated by FW, users must be authenticated and authorized. Test data is used on test or development systems, the possible unauthorized publication of which does not have a negative impact on the company. For testing, a special server is used with the use of virtualization, where the data is (if it makes sense) anonymized. Separate and temporary accesses are used for access to the test equipment, i.e. Access accounts are not identical to production access accounts.
Finding
Based on the observations, no deviation was found. AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.
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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Desatero pro uživatele

Description

The following evidence were provided:

- AV (ESET) is used in the organization.
- Users are prohibited from using software other than that provided to them by the IT service provider.
- Users have local admin privileges disabled on their workstations, they cannot intervene in the system.
- Information assets that can be attacked by malware (typically PC, NTB, Server, PDA, etc.) must be configured so that it is not possible to install unauthorized SW.
- Unnecessary network services are turned off.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti

Description

The following evidence were provided:

Subsequently, according to various rules, an e-mail notification arrives and vera.tovarkova@trianglprint.cz.
- A procedure for reporting violations to authorized bodies (security incident report,) is defined and established.
Reporting an incident
- A user who detects an event or incident is obliged to report this MKB immediately to email vera.tovarkova@trianglprint.cz
+420 606 939 180.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 6-1-3 Rizika_ISMS

Description

The following evidence were provided:

Potentially affected IT systems and software are identified, and assessed and any vulnerabilities are addressed during regular patches for company equipment. Vulnerability management is established on manual principles. The list of key assets for Patch management is based on Risk analysis. We made a Penetration test 1x12 months

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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: • SM 8-3-1 Standardy informacni bezpecnosti • ZA 6-1-3 Rizika_ISMS Description The following evidence were provided: Potentially affected IT systems and software are identified, and assessed and any vulnerabilities are addressed during regular patches for company equipment. Vulnerability management is established on manual principles. The list of key assets for Patch management is based on Risk analysis. We made a Penetration test 1x12 months
Finding
Based on the observations, no deviation was found. AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.
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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Topologie sítě

Description

The following evidence were provided:

Security network parameters are defined as:
- Turn off unnecessary services
- Securing access to resources and services (Authentication, Authorization, Accounting)
- User authentication (password)
- Logging of user activity
- Network division (employees x visit x customer data)
- Terminal protection (AV)
- Network protection against the user (allow only authenticated users to connect to the LAN)
- Antispoofing

There are 3 networks installed in the organization.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti

Description

The following evidence were provided:

Within the organization, a procedure for safe development is established for each project. These rules are an integral part of every project. It mainly concerns:
- There must be a separate environment (logical or physical) for testing, development, and production.
- All operating system installations must first be tested, primarily from the point of view of future use (burden, risks, etc.).
- Access to source code and libraries must be limited and based on a "need to know" requirement.
- Use of data in non-production environments (test and development) must comply with the rules below:
o Test data that is based on real data must be anonymized for testing purposes.
o If real data is used in the test, the same information security rules must be followed as for the production system.
o The handling and disposal of test data must be in accordance with internal and legal regulations.
- Source codes and libraries must be protected and maintained separately from executables and databases.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti

Description

The following evidence were provided:

The security of network services is an internal IT service.
Security network parameters are defined as:
- Turn off unnecessary services
- Securing access to resources and services (Authentication, Authorization, Accounting)
- User authentication (password)
- Logging of user activity
- Network division (employees x visit x customer data)
- Terminal protection (AV)
- Network protection against the user (allow only authenticated users to connect to the LAN)
- Antispoofing

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti

Description

The following evidence were provided:

The company uses external IT services. If necessary, the requirements must be met:
 - there must be an SLA
 - there must be an NDA contract
 - the contract must be approved by the Director-General
 - there must be a procedure for possible termination of service and erasure of data
 - IT is responsible for terminating external services

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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: • SM 8-3-1 Standardy informacni bezpecnosti Description The following evidence were provided: The company uses external IT services. If necessary, the requirements must be met: - there must be an SLA - there must be an NDA contract - the contract must be approved by the Director-General - there must be a procedure for possible termination of service and erasure of data - IT is responsible for terminating external services
Finding
Based on the observations, no deviation was found. AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.
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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 1-1-10 Hodnoceni dodavatelu

Description

The following evidence were provided:

Suppliers and cooperation partners are subjected to a risk assessment with regard to information security.
An appropriate level of information security is ensured by contractual agreements with suppliers and cooperation partners.
Suppliers and cooperation partners are contractually obliged to also pass on any requirements regarding an appropriate level of information security also to their subcontractors.

Based on the elaboration of the quality of suppliers, which is evaluated once a year, it is possible to change the supplier / contractor. Aspects of change in supplier services The following aspects should be considered:
- Changes to supply contracts
- Improving the existing services offered
- Development of new applications and systems
- Modify or update the organization's policies and procedures

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

Description: Contract with external IT supplier exists but is not formally signed.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- ZA 1-1-10 Hodnoceni dodavatelu
- Sample NDA

Description

The following evidence were provided:

Confidentiality or confidentiality agreements are an integral part of any contractual relationship. These agreements should always include:
- Definition of the information to be protected,
- Required actions when the contract is terminated
- Responsibilities
- Ownership of information, trade secrets, intellectual property,
- Permissible use of confidential information
- The right to audit and monitor activities
- The process of reporting and reporting unauthorized disclosure or leakage of information
- Expected step in case of breach of contractual agreement.

The NDA is reviewed regularly once every 12 months.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidence provided is ☒ plausible ☐ not plausible.

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Sample Employees contract
- ZA 7-1-4 Evidence právních požadavků a souladu

Description

The following evidence were provided:

- Prepared register of legal requirements, and planning measures.
- Intellectual property protection is dealt with contractually in each employment and supply contract.
- Records are stored on internal servers and in backups, access to records is restricted by access rights. There is a shredding and archiving procedure that defines the storage time of documentation.

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

Description: Register of legislative requirements exists, but shredding rules are not mentioned.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

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:

- SM 8-3-1 Standardy informacni bezpecnosti
- Podmínky ochrany osobnich udajů
- GDPR Dokumentace

Description

The following evidence were provided:

The organization has implemented a personal data protection policy, which is in accordance with Regulation No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals.

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

Description: GDPR documentation exists, but is not fully adjusted to the reality.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

Planned measures (including implementation period)

Evaluation at Follow-Up

8 Prototype Protection

The module has not been assessed.

9 Data protection

The module has not been assessed.