

Global Network Group

SOP.008

SERMI

Code: SOP.008
Approved by: GNG board
Version: V4 – Januari 2024
Status: APPROVED



1. Definitions

1.1

The in this document mentioned terms are defined in the RD.004 (EMCI Register list of terms and conditions).

1.2

Employees are seen as meaning IO's or RSS employees.

2. Purpose

2.1

This document clarifies certain work procedures that SERMI Register maintains for the SERMI scheme.

2.2

In case of SERMI inspections, SERMI Register follows as general guidance the documents of the SERMI organization and any guidance hereof.

2.3

This SOP is binding for clients and SERMI Register.

2.4

Wherever this document refers to a #UC, the relevant use case from the SERMI scheme is meant. This is seen as inserted and binding, SERMI Register will follow this. Where the Use Case specifies an output, this is the performance indicator that GNG must follow.

2.5

The management system documented in ID.003 and ID.004 means that GNG can and shall be responsible for the inspection of IOs and their respective IO employees and for issuing approval and authorization inspection certificates in accordance with Commission Delegated Regulation (EU) 2021/1244, and for revoking such certificates.

3. Digidentity and CETOOL

3.1.

Global Network Group maintains a formal relationship with Digidentity as Trust Center in accordance with #UC CA 1.

3.2.

CETOOL will be used exclusively, without choice for an alternative process, for all SERMI inspections.

3.3

Digidentity can be contacted at Sermi-support@digidentity.com for all reporting, queries and problems regarding SERMI.

4. SERMI Inspections

4.1.

Global Network Group, through SERMI Register will, perform inspections and issue certificates in accordance with the SERMI scheme. All inspections are done in strict accordance with the SERMI scheme and Annex X to Regulation (EU) 2018/858. In principle all inspections will be documented in CETOOL.

4.1.2

Before a certificate is issued GNG will follow up UC CA2 and require an initial remote inspection. PD.001 is used for this.

4.2

Before an onsite assessment the auditor does not need to setup a specific audit plan but will require access to the file of the IO and IO's listed in CETOOL, at least 7 days before this inspection this must be done.

4.2.

GNG will perform on site inspections (planned at least 3 months in advance internally) in accordance with #UC CA3: Onsite inspection.

4.2.1

During the onsite inspection GNG will check all related documents required by the SERMI scheme, establish compliance against the procedural requirements, and check that a legitimate business activity is pursued.

4.2.2.

GNG will also take a sample of client files to verify that the procedural requirements for security-related operations as defined in the SERMI scheme article 6.3.6. are followed. This includes that the documents required for the procedural steps are in order and that the repair order lists the value of the odometer and the reason for repair.

4.2.3.

The lead auditor is tasked with determining the required follow up plan in case of non-conformities in accordance with the GNG non-conformity scale as defined in article 4.2.4.

4.2.4.

The lead auditor is responsible for determining whether a non-conformity is minor (and may be resolved in accordance with article 4.12) or major.

4.2.5

During an onsite inspection GNG must verify that a legitimate business activity takes place and thus companies must comply with point 6.3 of Annex X of Regulation 2019/858. This will be done through asking of questions but may also be established in information or materials available online or in the company location.

4.3.

GNG will perform IO/RSS renewal inspections in accordance with #UC CA4 and will issue a paper certificate for the IO/RSS upon certification. GNG will follow up the notification obligations from #UC CA4 when needed. All onsite inspections must also be done in accordance with article 4.2. GNG will also issue a paper certificate to companies.

4.3.1

All inspection reporting will be done through CETOOL and the client will receive a CAPA report

4.4.

GNG will update certificates in accordance with #UC CA 5 and #UC CA 10 (in the case of Employees) but must receive a written request (email) to do so by the client.

4.5.

Each employee that will receive a certificate must be inspected in accordance with #UC CA6. This does not mean that during a physical inspection all employees must be present, in accordance with point 2 of the sanctioned interpretation list.

4.6.

GNG will perform pseudonymization of personal data in accordance with #UC CA7. This will be done within CETOOL, automatically or manually in the certificate IO/RSS employee function.

4.7.

GNG will implement #UC CA8 and will communicate with the Trust Center (see article 3) through CETOOL. A signed agreement and test has been performed to validate this.

4.8.

GNG will inspect an employee for renewal in accordance with #UC CA 9. Reminders will be handled via CETOOL.

4.9

GNG will maintain a complaints procedure and will process complaints in accordance with this procedure, and thus by this implementing #UC CA11. All complaints must be filled in using FO.002 found on the SERMI Register website.

4.10

For complaints concerning the approval of IO/RSS or employee GNG will implement #UC CA 12 and #UC CA 13. Any assessment in accordance with these use cases must be done by a different auditor who performed the initial assessment of the IO/RSS or employee. It is up to GNG to decide what actions to in relation to complaints vis-à-vis a re-audit of the SERMI requirements.

4.11

Every quarter GNG will provide statistics of the SERMI organization and the European Commission in accordance with #UC CA 14.

4.12

IOs/RSSs and IO/RSS employees that have received a negative inspection result may provide GNG with additional information correcting minor deficiencies within 15 working days from receiving the negative inspection result. CABs shall accordingly determine whether the inspection result is to be changed.

4.13.

FO.006 must be signed by the IO/RSS.

5. Rules and responsibilities

In accordance with the rules from the SERMI scheme GNG, in accordance with PD.004, MS.000, MS.001 and the above:

- Shall keep the data submitted for the approval of an IO/RSS at all times. GNG may, if desired, delete specific personal ID card but must keep confirmed copies of the assessment results confirming explicitly that such personal data was indeed audited.
- Shall establish a secure communication channel with the TC and provide the inspection results to the TC in order for the TC to issue the security token with a digital certificate, this is done through Digidentity.
- Shall notify IO/RSS employees 6 months before authorization expires. The certification advice will include this date.
- Shall maintain a database containing data submitted for the authorization of IO/RSS employees, this is done in CETOOL.
- Shall communicate, within reasonable time, the inspection results concerning the IO/RSS or employees to the TC if GNG refuses to approve an IO/RSS or authorize of an IO/RSS employees, this shall be done through the CETOOL. GNG shall also communicate these results to CAB's in the same country.
- Shall only collect and use data required for the approval or authorization process;
- Shall keep all data relating to IO/RSS and IO/RSS employees confidential and shall ensure that only authorized employees have access to such data;
- Shall provide once a year statistics on the number of approval and authorizations issued and also on the number of refusals to SERMI and the Commission;
- Shall retain secure records of approval and authorization inspections for a period of 5 years – in accordance with point 1.
- Shall inform all other CABs in the Member State in which it is established about negative inspection results of an IO/RSS. CAB's shall be informed via email.
- Shall notify IOs/RSSs 6 months before their approval expires;
- Shall make random and unannounced on-site checks of IOs/RSSs within the 60 months approval validity period, and subject each approved IO/RSS to at least one random, on-site inspection over the 60 months approval validity period (minimum of 2 inspections: one random and one 6 months before authorization is due to expire). This shall be scheduled at the start of the certification process.
- Shall, on the basis of a complaint against an approved IO/RSS or an authorized IO/RSS employee, check that the concerned IO/RSS or IO/RSS employee are in compliance with the criteria against which they were respectively approved or authorized. The CAB shall determine during its investigation whether an on-site inspection is required;
- May, for the purpose of on-site inspections, request the assistance of market surveillance authorities from the Member State they are established.
- Shall revoke IO/RSS approvals and IO/RSS employee authorizations where they no longer comply with the criteria against which they were respectively approved or authorized.

6. Sanctioned interpretation list

6.1

In accordance with the rules from the SERMI scheme GNG will at all times apply the sanctioned interpretation list that can be found at <http://www.vehiclesermi.eu>.

6.2

In anticipation of further developments GNG will also adopt the interpretations listed in Annex 1 in its conformity assessment to provide clarity in conformity assessment. Annex 1 may be freely updated or amended depending on the developments in the SERMI scheme.

Annex 1

1.1

What is acceptable evidence of working in the automotive area?

To apply to become an Independent Operator (IO) you must provide evidence of working in the automotive area. This can be demonstrated by providing one of the following from the list below:

- Chamber of Commerce registration with SBI code related to the automotive sector combined
- A requested selection of invoices from your last three months of trading demonstrating repair and maintenance of motor vehicles.
- Current membership as an RDW workshop or a known and proven automotive umbrella organization (ie Bovag). Or the garage's status as part of a franchise (ie Bosch car service).
- Proven trackrecord on social media
- Other evidence at the discretion of GNG.

1.2

What is acceptable evidence of business ownership?

A registration from the chamber of commerce showing the ownership of the company and the registered directors. An overview of shareholders and directors (if legal entities) in the form of legal persons must be additionally documented.

1.3

What type of insurance policy is needed?

An insurance policy covering business activities to a range of at least EUR 1.5 million where EUR 1 million is for bodily damages and EUR 0.5 million is for property damages. In principle an insurance policy covering business activities for a minimum of EUR 1.5 million is sufficient.

It is also sufficient to have an insurance policy covering EUR 1 million for bodily damages and an insurance policy covering EUR 0.5 million for property damages. These can then be separate policies or 2 amounts covered under a single policy.

1.4

What data must be retained for at least 5 years after the work order?

All information relating to the process requirements of SERMI (identification of vehicle, owner, establishing of authority and the work order) must be kept for at least 5 years after the work order is issued. Personal data, like copies of ID cards, can be anonymized or an assessment report can be kept instead proving that you did verify you did check the ID card information before accepting the repair order.

1.5

How do you prove a lack of Criminal Record for the IO/RSS

Please provide a qualifying police clearance for the IO/RSS legal representative or in countries where possible a police clearance on the legal entity or the UBOs.

In countries where a police clearance is not possible a signed statement is needed.

Annex 2 Audit work procedure initial inspection article 4.4.

Article	What	Description
4.4.	Requirement	Role of the IOs
4.4.1.	Requirement	Responsibilities and requirements
4.4.1. (a)	Requirement	IOs shall request an inspection from their CAB to obtain approval
	Question	Is there an application form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, stop the audit, mark as Major non-conformity
4.4.1. (b)	Requirement	IOs shall inform their CAB about changes in their contact details
	Question	Have there been any changes in the present contact details send via email or other contact / indication? Does the website list other contact details as indicated and are these the new contact details?
	Allowed answer	No, mark as such in CE tool.
	Other answer(s)	Yes, with correct full details, adjust details where necessary and mark as such in CE tool
	Other answer(s)	Yes, however with incomplete details, mark as minor in CE tool and have IO/RSS send in the complete new details
4.4.1. (c)	Requirement	IOs shall inform their CAB when their business is dissolved
	Question	Has there been an email or other contact / indication notifying that the business has been dissolved?
	Allowed answer	No, mark as such in CE tool
	Other answer(s)	Yes, stop the audit, mark as Major non-conformity
4.4.1. (d)	Requirement	IOs shall record every security related RMI transaction and operation
	Question	Has the IO/RSS legal representative signed the contract noting that he is aware he needs to record RMI the transaction and operation for 5 years?
	Allowed answer	YES, mark as such in CE tool
	Other answer(s)	No, stop the audit, mark as Major non-conformity
4.4.1. (e)	Requirement	IOs shall inform their CAB of any termination of employment of any of their authorized employees
	Question	Has the IO/RSS informed the CAB of any terminations of employment of any of their authorized employees?
	Allowed answer	No, and no violation has been found, mark as such in CE tool
	Allowed answer	Yes, message was received within 3-days of termination and is processed / being processed, AND there are other approved employees
	Other answer(s)	Yes, message was not received within 3-days of termination, stop the audit, mark as Major non-conformity
	Other answer(s)	No, AND a violation has been found, stop the audit, mark as Major non-conformity
	Other answer(s)	Yes, message was received within 3-days of termination and is processed / being processed BUT there are no other approved employees, stop the audit, mark as Major non-conformity
4.4.1. (f)	Requirement	IOs shall report to the relevant authorities any offence or misconduct that has been committed by their authorized employees and that concerns security related RMI
	Question	Has there been a report of offence or misconduct from IO's/RSS regarding their employees and security related RMI?
	Allowed answer	No, mark as such in CE tool
	Allowed answer	Yes, revoke authority of authorized employee, investigate where needed. If there are more authorized employees than have no reports the audit can continue, mark as such in CE tool

Article	What	Description
	Other answer(s)	Yes, revoke authority of authorized employee. If no more employees, stop the audit, mark as Major non-conformity
4.4.1. (g)	Requirement	<i>IOs shall ensure that their authorized employees only use their own authorization inspection certificates</i>
	Question	Has the IO/RSS legal representative signed the contract informing him of the clause?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, stop the audit, mark as Major non-conformity
4.4.1. (h)	Requirement	<i>IOs shall ensure that all fees relating to their IO employee's authorization have been paid</i>
	Question	Have all IO/RSS invoices from CAB been paid?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and inform IO/RSS the invoice needs to be paid before continuation of process
4.4.1. (i)	Requirement	<i>IOs shall ensure that their IO employees are trained for repair activities concerning automotive maintenance, reprogramming and security and safety functions</i>
	Question	Are training certificates for all IO/RSS employees mentioned in the list conform Regulation 2021/1244 clause 4.3.3.B present and do they conform to the requirements of SERMI Sanctioned interpretations list?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and inform IO/RSS the certificate(s) need(s) to be send before continuation of process
4.4.1. (j)	Requirement	<i>IO shall request their CAB for an on-site inspection in the six months prior to the expiration of their approval inspection certificate</i>
	Question	Has the IO/RSS and CAB agreed on a date for the on-site inspection 6 months prior to expiration of certification?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and inform IO/RSS the Date needs to be planned and confirmed.

Annex 3 Audit work procedure on-site inspection article 4.4.

Article	What	Description
4.4.	Requirement	Role of the IOs
4.4.1.	Requirement	Responsibilities and requirements
4.4.1. (a)	Requirement	IOs shall request an inspection from their CAB to obtain approval
	Question	Request during inspection if there is approval from IO for the inspection being performed by CAB via a question with allowed answers.
	Allowed answer	Yes
	Other answer(s)	No, stop the audit, mark as Major non-conformity
4.4.1. (b)	Requirement	IOs shall inform their CAB about changes in their contact details
	Question	Request during inspection if there have been any changes in the present contact details via a question with allowed answers.
	Allowed answer	No, mark as such in CE tool.
	Other answer(s)	Yes, mark as minor in CE tool and have IO/RSS send in the new details
4.4.1. (c)	Requirement	IOs shall inform their CAB when their business is dissolved
	Question	Request during inspection if the IO/RSS has been dissolved or is in the process of being dissolved via a question with allowed answers.
	Allowed answer	No, mark as such in CE tool
	Other answer(s)	Yes, stop the audit, mark as Major non-conformity
4.4.1. (d)	Requirement	IOs shall record every security related RMI transaction and operation
	Question	Request during inspection if all security related RMI transactions and operations have been logged and that the legal representative is aware he needs to keep all data for 5 years via a question with allowed answers. Additionally compliance will be demonstrated by sampling all work orders of the IO/RSS as per the below.
	Allowed answer	Yes, check the relevant RMI requirements in the SERMI Scheme elements 6.3.6. If the logged data conforms the requirements of SERMI Scheme elements 6.3.6. Mark as such in CE tool
	Other answer(s)	No, stop the audit, mark as Major non-conformity
	Other answer(s)	Yes, however relevant RMI requirements in the SERMI scheme 6.3.6 are not met, stop the audit. Mark as Major non-conformity.
	Other answer(s)	Yes, AND relevant RMI requirements are met however not all orders are stored, stop the audit. Mark as Major non-conformity.

Article	What	Description
	Note:	<p>On the work order / RMI documentation there needs to be the following information or a reference to a document with the following information:</p> <p>Customer ID card, passport, drivers license or roadside membership card. Where possible the following information must be registered. The IO/RSS must ensure the Identity information is stored in a way which can be audited:</p> <ul style="list-style-type: none"> o Name and surname of the customer o Identity card/passport number and/or number of the roadside member card o Fleet management or rental car company name o Contact name of the respective company o Address of the respective company o Telephone number of the respective company o Driver's company identification <p>This additional information is requested in the circumstances where the customer will not have vehicle registration documents:</p> <ul style="list-style-type: none"> o Fleet management o Rental Cars o Loan <p>If vehicle registration documents are available, the Vehicle VIN has to be registered as well as the vehicle registration number. The VIN of the vehicle registration must be checked and be the same as the vehicle VIN. This must show from the documentation,</p> <ul style="list-style-type: none"> • Additional information to be noted should be: <ul style="list-style-type: none"> o Registration number A o Make D.1 o Type, variant, version D.2 • Additional information registered on the documentation should be: <ul style="list-style-type: none"> o The reason of repair. o The Odometer setting. o Signature of the customer and the owner(s). Where this is different all signatures need to be present. <p>The mechanic carrying out the audit should be one of the certified IOE's/RSSe's. Work orders sampled must check that other employees are not carrying out SERMI work.</p> <p>A sample of all work orders over the certification period must be requested and this must be proportionally spread over the time period since issuance of the certificate.</p> <p>Sampling can be done by using for example the Square root methodology.</p>
4.4.1. (e)	Requirement	<i>IOs/RSSs shall inform their CAB of any termination of employment of any of their authorised employees</i>
	Question	Request during inspection if the IO/RSS has any terminations of employment of any of their authorized employees via a question with allowed answers.?
	Allowed answer	No, and no violation has been found, mark as such in CE tool
	Allowed answer	Yes, message was received within 3-days of termination

Article	What	Description
	Other answer(s)	Yes, message was not received within 3-days of termination, stop the audit, mark as Major non-conformity
	Other answer(s)	No, AND a violation has been found, stop the audit, mark as Major non-conformity
4.4.1. (f)	Requirement	<i>IOs/RSSs shall report to the relevant authorities any offence or misconduct that has been committed by their authorised employees and that concerns security related RMI</i>
	Question	Request during inspection if there has been a report of offence or misconduct from IO's/RSS regarding their employees in relation with the security related RMI via a question with allowed answers.
	Allowed answer	No, mark as such in CE tool
	Allowed answer	Yes, revoke authority of authorized employee, investigate where needed. If there are more authorized employees than have no reports the audit can continue, mark as such in CE tool
	Other answer(s)	Yes, revoke authority of authorized employee. If no more employees, stop the audit, mark as Major non-conformity
4.4.1. (g)	Requirement	<i>IOs/RSSs shall ensure that their authorized employees only use their own authorization inspection certificates</i>
	Question	Check the relevant RMI logs and work orders for deviations from login and performance of maintenance via a question with allowed answers. Additionally ask present employees if they share their codes.
	Allowed answer	No deviation has been found, mark as such in CE tool.
	Other answer(s)	Deviation(s) is(are) found, stop the audit, mark as Major non-conformity
4.4.1. (h)	Requirement	<i>IOs shall ensure that all fees relating to their IO employee's authorization have been paid</i>
	Question	Have all IO/RSS invoices from CAB been paid? Check internally and ask the Legal Representative via a question with allowed answers.
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and inform IO/RSS the invoice needs to be paid before continuation of process. IF no payment after 15 days, mark as major and stop the audit.
4.4.1. (i)	Requirement	<i>IOs/RSSs shall ensure that their employees are trained for repair activities concerning automotive maintenance, reprogramming and security and safety functions</i>
	Question	Are training certificates for all IO/RSS employees mentioned in the list conform Regulation 2021/1244 clause 4.3.3.B present and do they conform to the requirements of SERMI Sanctioned interpretations list?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and inform IO/RSS he needs to have this documentation available at all times.
4.4.1. (j)	Requirement	<i>IO shall request their CAB for an on-site inspection in the six months prior to the expiration of their approval inspection certificate</i>
	Question	Has the IO/RSS and CAB agreed on a date for the on-site inspection 6 months prior to expiration of certification? Is the legal representative aware of this responsibility? Verify via a question with allowed answers.
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and inform IO/RSS the Date needs to be planned and confirmed

Annex 4 Audit work procedure initial inspection article 4.5.

Article	What	Description
4.5.	Requirement	Role of the employees
4.5.1.	Requirement	Responsibilities and requirements
4.5.1. (a)	Requirement	IO/RSS employees shall request their CAB for authorization
	Question	Has the IO/RSS Employee signed and sent in his 4.5.1 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (b)	Requirement	IO/RSS employees shall register themselves on the vehicle manufacturer's RMI system
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (c)	Requirement	IO/RSS employees shall access security-related RMI in accordance with EN ISO standard 18541 – 2014
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (d)	Requirement	IO employees shall ensure that all records of security related RMI downloaded from the vehicle manufacturer RMI system shall not be stored any longer than necessary for performing the operation for which the information is needed
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (e)	Requirement	where applicable, IO employees shall notify their IO employer that their digital certificate is no longer required
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (f)	Requirement	IO employee shall not share with any third party the security token, the digital certificate or the PIN
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (g)	Requirement	IO employees shall be responsible for using the personal security token and PIN correctly
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (h)	Requirement	IO employees shall inform their IO and their TC about any loss or misuse of their security token within 24 hours of such loss or misuse
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.
4.5.1. (i)	Requirement	IO employees shall report to the relevant authorities any request or act from other IO employees relating to security-related RMI that does not constitute a legitimate business activity as referred to in point 6.3 of this Annex
	Question	Has the IO/RSS Employee signed and send in his 4.5 responsibilities form?
	Allowed answer	Yes, mark as such in CE tool

Article	What	Description
	Other answer(s)	No, mark as minor in CE tool and have IO/RSS employee(s) send in the new details.

Annex 5 Audit work procedure on-site inspection article 4.5.

Article	What	Description
4.5.	Requirement	Role of the employees
4.5.1.	Requirement	Responsibilities and requirements
	Instruction	<ul style="list-style-type: none"> Please note that conform the SERMI sanctioned interpretations list not all employees must be present during the on-site inspection. Below is only for present and available employees. If at the end of the on-site inspection no IO/RSS employees can be approved. The audit is to be stopped and this is to be marked as a major non-conformity. If there are approvals to be revoked this must be marked as a minor non-conformity. Only after all approvals are revoked can the IO/RSS certification be completed.
4.5.1. (a)	Requirement	IO employees shall request their CAB for authorization
	Question	Is there approval from IO/RSS employees for the inspection being performed by CAB. Verify via a question with allowed answers.
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, this (these) employee(s) is (are) not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (b)	Requirement	IO employees shall register themselves on the vehicle manufacturer's RMI system
	Question	Has the IO Employee registered themselves on the relevant manufacturer RMI system and is he aware of how the login works? Verify via a question with allowed answers. <u>Note</u> This can be checked by having the IO/RSS employee login using his own certification as a demonstration.
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, this (these) employee(s) is (are) not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (c)	Requirement	IO employees shall access security-related RMI in accordance with EN ISO standard 18541 – 2014
	Question	Is the IO Employee able to access security-related RMI in accordance with EN ISO standard 18541 – 2014? Verify via a question with allowed answers. <u>Note</u> This can be checked by having the IO/RSS employee login using his own certification.
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, this (these) employee(s) is (are) not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (d)	Requirement	IO employees shall ensure that all records of security related RMI downloaded from the vehicle manufacturer RMI system shall not be stored any longer than necessary for performing the operation for which the information is needed

	Question	Can the IO/RSS employee show that the records of security related RMI downloaded from the vehicle manufacturer RMI system are not stored longer than necessary? Verify via a question with allowed answers. <u>Note</u> He/She can do this by showing storage and download files and the cache?
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, this (these) employee(s) is (are) not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (e)	Requirement	where applicable, IO employees shall notify their IO employer that their digital certificate is no longer required
	Question	Has the IO/RSS employee informed the IO/RSS employer that their digital certificate is no longer needed? Verify via a question with allowed answers.
	Allowed answer	No, AND no violation has been found, mark as such in CE tool.
	Allowed answer	Yes, message to CAB from IO/RSS employer was received within 3-days of termination where applicable.
	Other answer(s)	Yes, message to CAB from IO/RSS employer was not received within 3-days of termination where applicable, employee is not to be counted as evaluated employee, relevant approvals need to be revoked.
	Other answer(s)	No, AND a violation has been found, employee is not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (f)	Requirement	IO employee shall not share with any third party the security token, the digital certificate or the PIN
	Question	Ask the IO/RSS employee if he has shared the security token, the digital certificate or the PIN with a third party? Verify via a question with allowed answers.
	Allowed answer	No, mark as such in CE tool
	Other answer(s)	Yes, this employee is not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (g)	Requirement	IO employees shall be responsible for using the personal security token and PIN correctly
	Question	Does the IO/RSS employee know how to use the personal security token and PIN correctly? <u>Note</u> Have the employee login to show this.
	Allowed answer	Yes, mark as such in CE tool
	Other answer(s)	No, this employee is not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (h)	Requirement	IO employees shall inform their IO and their TC about any loss or misuse of their security token within 24 hours of such loss or misuse
	Question	Ask the IO employee if he has lost the security token or if this has been misused? Verify via a question with allowed answers.
	Allowed answer	No, mark as such in CE tool
	Allowed answer	Yes, however the comment has been made to CAB within 24 hours of the misuse. <u>Note</u> In this case, the employees authorization with TC needs to be reset as soon as possible.

	Other answer(s)	Yes, AND no comment has been made to the CAB and relevant authorities within 24 hours, employee is not to be counted as evaluated employee, relevant approvals need to be revoked.
4.5.1. (i)	Requirement	<i>IO employees shall report to the relevant authorities any request or act from other IO employees relating to security-related RMI that does not constitute a legitimate business activity as referred to in point 6.3 of this Annex</i>
	Question	Have IO/RSS employees received any request or act from other IO employees relating to security-related RMI that does not constitute a legitimate business activity as referred to in point 6.3 of Regulation 2021/1244? Verify via a question with allowed answers.
	Allowed answer	No, mark as such in CE tool
	Allowed answer	Yes, however CAB and relevant authorities has been informed and correction action has been taken to the satisfaction of the relevant authorities.
	Other answer(s)	Yes, AND CAB and relevant authorities have not been informed and correction action has not been taken to the satisfaction of the relevant authorities, employee is not to be counted as evaluated employee, relevant approvals need to be revoked.