

*e.PN –
e.solutions Partner Network*

e.PN InfoSec Audit

Purpose of the e.PN InfoSec Audit

- *Purpose*

- Requirements of the customer for information security (TISAX[®] / ISO 27001)
- Contractual obligations of partner companies for information security
- Focus on chosen connectivity solutions (Internet, e.PN.Client + e.PN.VPN , e.PN VDI, e.PN.Connect)
- Consideration of physical security due to the use of targets (prototype components).

- *Brief overview of recognized standards for information security:*

- TISAX[®] (Trusted Information Security Assessment Exchange)
 - An assessment and exchange mechanism of the automotive industry for information security.
 - The implementation is based on the VDA ISA catalogue.
- ISO 27001
 - International standard of information security; basic requirements for an information security management system

Key Facts of e.PN InfoSec Audit

• *Scope of the audit*

- The e.PN audit is based on the VDA ISA requirements
- The duration and type of implementation depend on the collaboration use case as well as the connectivity technology.

Effort and duration of implementation 

With TISAX® Labels

- Shared Results within ENX Portal
 - Detail Level: A+ Labels
- Completed questionnaire "Physical Security" (depending on label and use case)
- Possibly short (telephone) discussion

With ISO 27001 certification

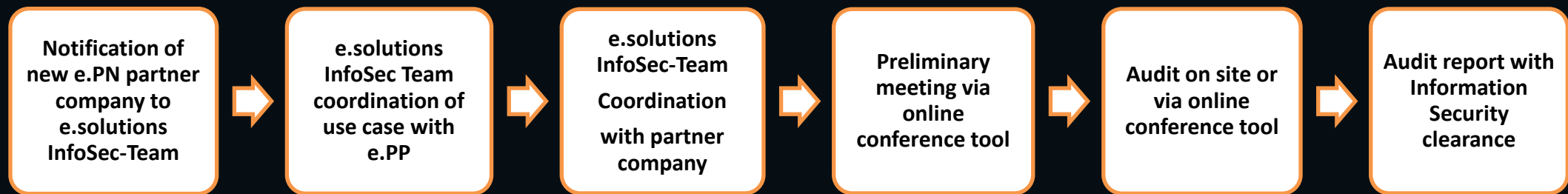
- Copy of the certificate + scope
- Completed questionnaire "Physical Security"
- If required, evidence in the form of policies / proof of implementation
- Possibly short (telephone) discussion

Without certification

- Completed VDA ISA "Information Security" and "Prototype Protection"
- Completed questionnaire "Physical Security"
- Short audit (on a sample basis)

Schematic Process of the e.PN InfoSec Audit

- The following descriptions apply to partner companies without certificates in the area of information security*



Audit focus on technologies, use case and connection type

Security clearance check with action plan if necessary

Procedure of Preliminary Meeting

Duration: ca. 60 min

Introduction

Explanation of the
questionnaires

Procedure of the
e.PN InfoSec Audit

Involved parties:

e.solutions:

Information Security Manager
other rolls as needed

Partner company:

Information Security Officer
if necessary responsible IT-personnel
if necessary Account Manager

Possible Audit Agenda

Topic	Content	Participants of Partner Company
Kick-Off	Introduction, explanation procedure of the audit	<ul style="list-style-type: none">• Account Manager• CEO• IT-personnel• Information Security Officer
Physical security	Discussion about questionnaire	<ul style="list-style-type: none">• Account Manager• IT-personnel• Information Security Officer
VDA ISA questionnaire	Discussion about questionnaire (randomly)	<ul style="list-style-type: none">• Account Manager• IT-personnel• Information Security Officer
On-site check	On-site check	<ul style="list-style-type: none">• Account Manager• IT-personnel• Information Security Officer
Closing meeting	Summary and next steps	<ul style="list-style-type: none">• Account Manager• CEO• IT-personnel• Information Security Officer

Partner Company Connection Technologies

- *Rules*

- All connection technologies take place according to „need-to-know“ principle
- company regulations apply

- *The following technologies are possible:*

- Internet
- e.PN.VPN & e.PN.Client (e.solutions-Laptop with VPN-Client)
- e.PN VDI (Virtual Desktop Infrastructure)
- e.PN.Connect (VPN direct connection)

- *Notes*

- Various services can be accessed via the different possibilities
- The required service determines the connection to be set up
- Connection technologies can be combined with each other
- e.PP must define the required connection technology together with e.PN support
- Clarify technical requirements with ePN-support@esolutions.de

Audit Checklist/Required Questionnaires

✓ Completed questionnaire VDA ISA (latest version)VDA ISA (latest version)

- „Information Security“ and „Prototype Protection“ with maturity level, implementation description and reference documentation.

✓ Completed questionnaire „Physical Security“

Questions and Contact

*If you have any questions about e.PN InfoSec Audit, please
do not hesitate to send us an E-Mail*

[*eso.Group.Informationssicherheit@esolutions.
de*](mailto:eso.Group.Informationssicherheit@esolutions.de)

Thank you!