

# *e.PN – e.solutions Partner Netzwerk*

## e.PN InfoSec Audit

Informationssicherheit

e.solutions GmbH

# Zweck des e.PN InfoSec Audits

- *Zweck*

- Anforderungen der Auftraggeber an Informationssicherheit (TISAX® / ISO 27001)
- Vertragliche Verpflichtung der Partnerfirmen an Informationssicherheit
- Fokus auf ausgewählte Anbindungstechnologie (Internet, e.PN.Client + e.PN.VPN, e.PN VDI, e.PN.Connect)
- Berücksichtigung der physischen Sicherheit aufgrund der Verwendung von Targets (Komponenten der Prototypen)

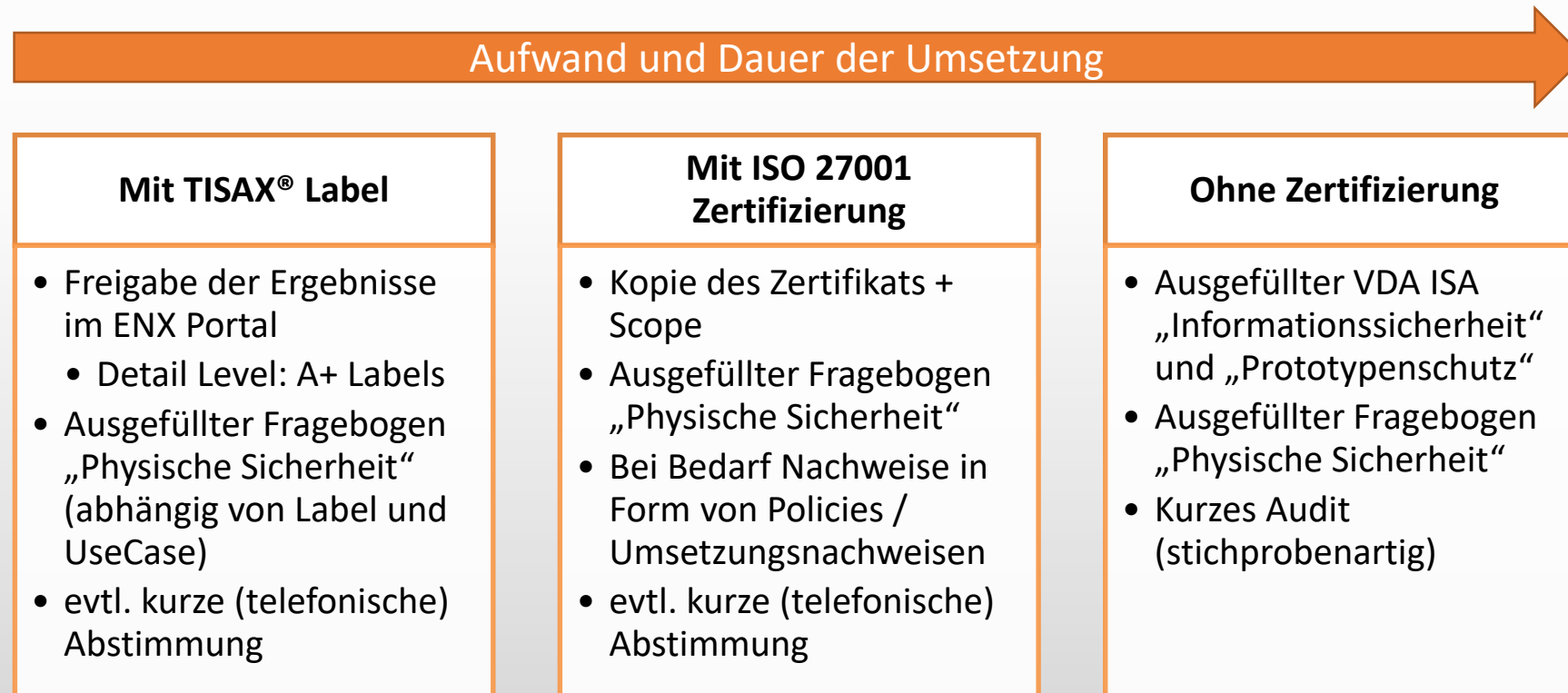
- *Kurzüberblick anerkannter Standards / Prüfung der Informationssicherheit*

- TISAX® (Trusted Information Security Assessment Exchange)
  - Ein Prüf- und Austauschmechanismus der Automobilindustrie für Informationssicherheit. Die Durchführung basiert auf dem VDA ISA Katalog.
- ISO 27001
  - Internationaler Standard der Informationssicherheit; Grundlegende Anforderungen an ein Informationssicherheitsmanagementsystem

# Eckpunkte des e.PN InfoSec Audits

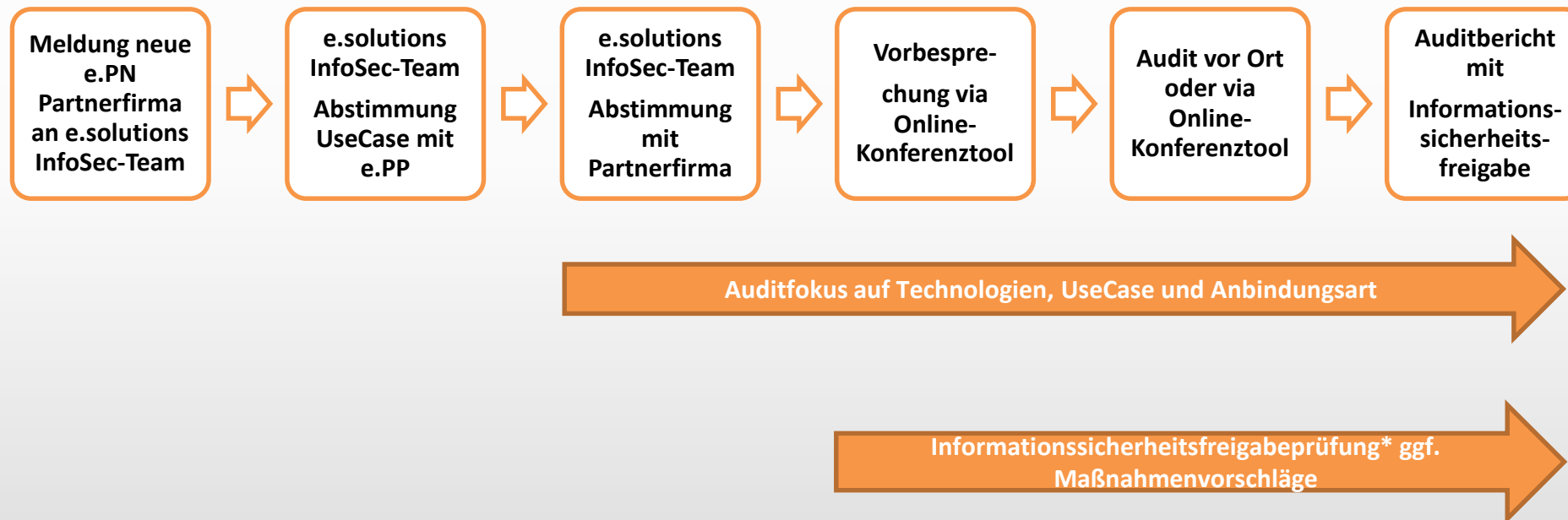
## • Umfang des Audits

- Das e.PN Audit basiert auf den VDA ISA Anforderungen
- Dauer und Art der Umsetzung sind abhängig von dem UseCase der Zusammenarbeit sowie der Anbindungstechnologie.



# Schematischer Ablauf des e.PN InfoSec Audits

- Die nachfolgenden Beschreibungen gelten für Partnerfirmen ohne Zertifikate im Bereich der Informationssicherheit



\*Prüfung gemäß VDA ISA und physische Sicherheit durch e.solutions

# Ablauf der Vorberechung

Dauer: ca. 60 min

Vorstellung

Erläuterung der  
Fragebögen

Ablauf des e.PN  
InfoSec Audit

## Beteiligten:

e.solutions	Information Security Manager Andere Rollen nach Bedarf
Partnerfirma	Informationssicherheits-Verantwortliche ggf. IT-Verantwortliche ggf. Account Manager

# Mögliche Auditagenda

Thema	Inhalt	Teilnehmer der Partnerfirma
Kick-Off	Vorstellung, Ablauf des Audits	<ul style="list-style-type: none"><li>• Account Manager</li><li>• Geschäftsführer</li><li>• IT Verantwortliche</li><li>• Informationssicherheits-Verantwortliche</li></ul>
Physische Sicherheit	Diskussion zum Fragebogen	<ul style="list-style-type: none"><li>• Account Manager</li><li>• IT Verantwortliche</li><li>• Informationssicherheits-Verantwortliche</li></ul>
VDA ISA Fragebogen	Diskussion zum Fragebogen (stichprobenartig)	<ul style="list-style-type: none"><li>• Account Manager</li><li>• IT Verantwortliche</li><li>• Informationssicherheits-Verantwortliche</li></ul>
Ortsbegehung	Rundgang am Standort	<ul style="list-style-type: none"><li>• Account Manager</li><li>• IT Verantwortliche</li><li>• Informationssicherheits-Verantwortliche</li></ul>
Abschlussbesprechung	Zusammenfassung und nächste Schritte	<ul style="list-style-type: none"><li>• Account Manager</li><li>• Geschäftsführer</li><li>• IT Verantwortliche</li><li>• Informationssicherheits-Verantwortliche</li></ul>

# Partner Anbindungstechnologien

- *Regeln*

- Alle Anbindungen erfolgen nach dem „need-to-know“ Prinzip
- Firmenregelungen gelten

- *Folgende Technologien sind möglich:*

- Internet
- e.PN.VPN & e.PN.Client (e.solutions-Laptop mit VPN-Client)
- e.PN VDI (Virtual Desktop Infrastructure)
- e.PN.Connect (VPN Direktanbindung)

- *Hinweise*

- Über die verschiedenen Wege sind verschiedene Dienste erreichbar
- Der benötigte Dienst bestimmt die einzurichtende Anbindung
- Anbindungstechnologien sind miteinander kombinierbar
- e.PP muss die erforderliche Anbindungstechnologie mit dem e.PN-Support festlegen
- Technische Anforderungen mit [ePN-support@esolutions.de](mailto:ePN-support@esolutions.de) klären

# *Audit Checkliste – erforderliche Unterlagen*

## *✓ Ausgefüllter Fragebogen VDA ISA (aktuellste Version)*

- „Informationssicherheit“ und „Prototypenschutz“ mit Bewertung des Reifegrads, Beschreibung der Umsetzung und Referenzdokumentation.

## *✓ Ausgefüllter Fragebogen „Physische Sicherheit“*



# Kontakt



[eso.group.informationssicherheit@esolutions.de](mailto:eso.group.informationssicherheit@esolutions.de)

- Bei Fragen zum Thema e.PN InfoSec Audit, zögern Sie bitte nicht uns eine Email zu senden.

Vielen Dank!