T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Frankfurt a.M., 10. - 11.11.2016

Informationssicherheit beim Datenaustausch

Dr. Ingolf Menzel
operational services

OPERATIONAL SERVICES
YOUR ICT PARTNER

INFORMATIONSSICHERHEIT

Ein Praxisbericht

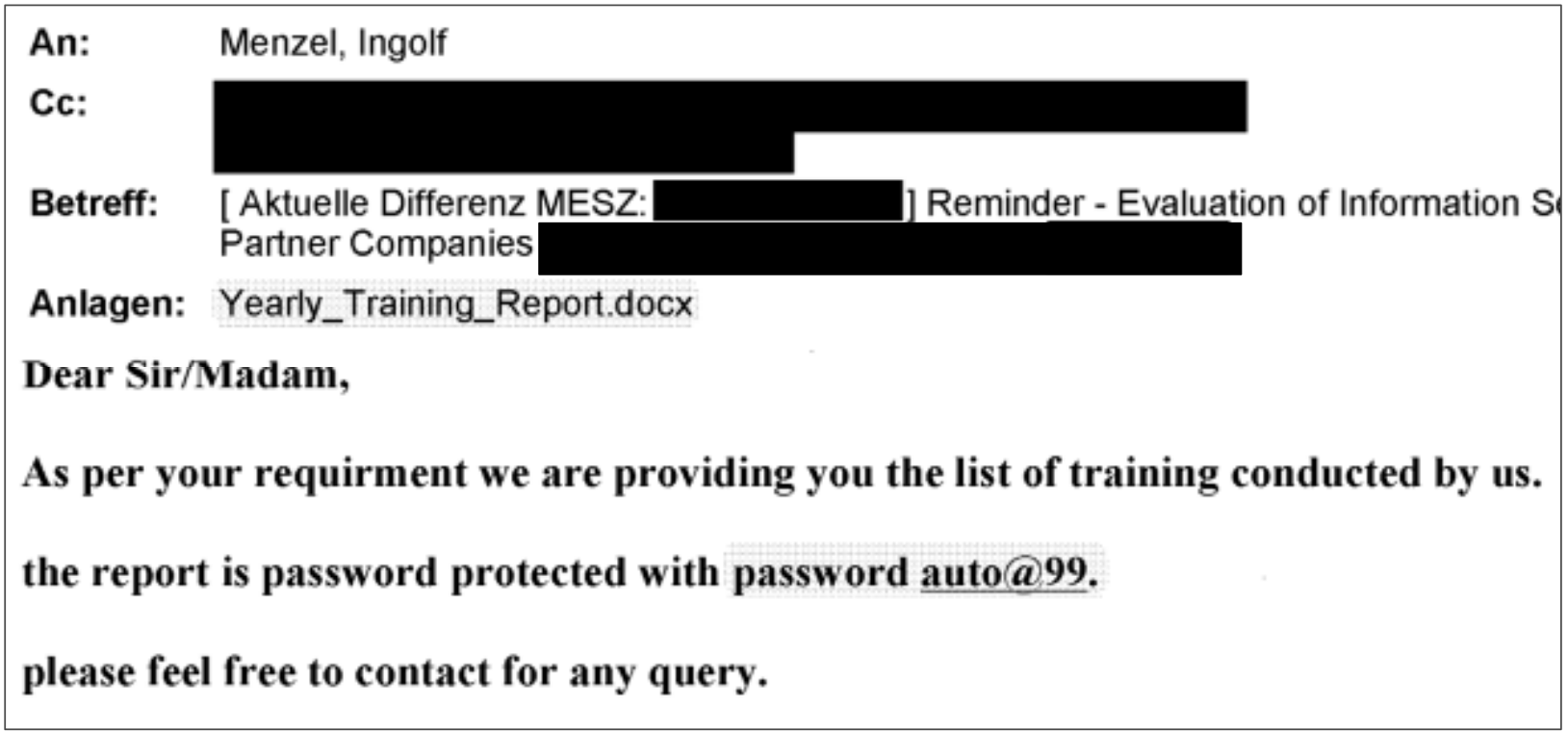
Dr. Ingolf Menzel

INFORMATIONSSICHERHEIT BEIM DATENAUSTAUSCH

Überblick zu den Anforderungen und Auditierung deren Umsetzung
Eine kleine Einführung mit Praxisbericht

SICHERE KOMMUNIKATION?

Vertrauliche Information angefordert und erhalten



An: Menzel, Ingolf

Cc: [redacted]

Betreff: [Aktuelle Differenz MESZ: [redacted]] Reminder - Evaluation of Information S
Partner Companies [redacted]

Anlagen: Yearly_Training_Report.docx

Dear Sir/Madam,

As per your requirment we are providing you the list of training conducted by us.

the report is password protected with password auto@99.

please feel free to contact for any query.

INFORMATIONEN ERFOLGREICH GESCHÜTZT?

AUTO SHANGHAI

Jiangling Motor “Landwind X7”

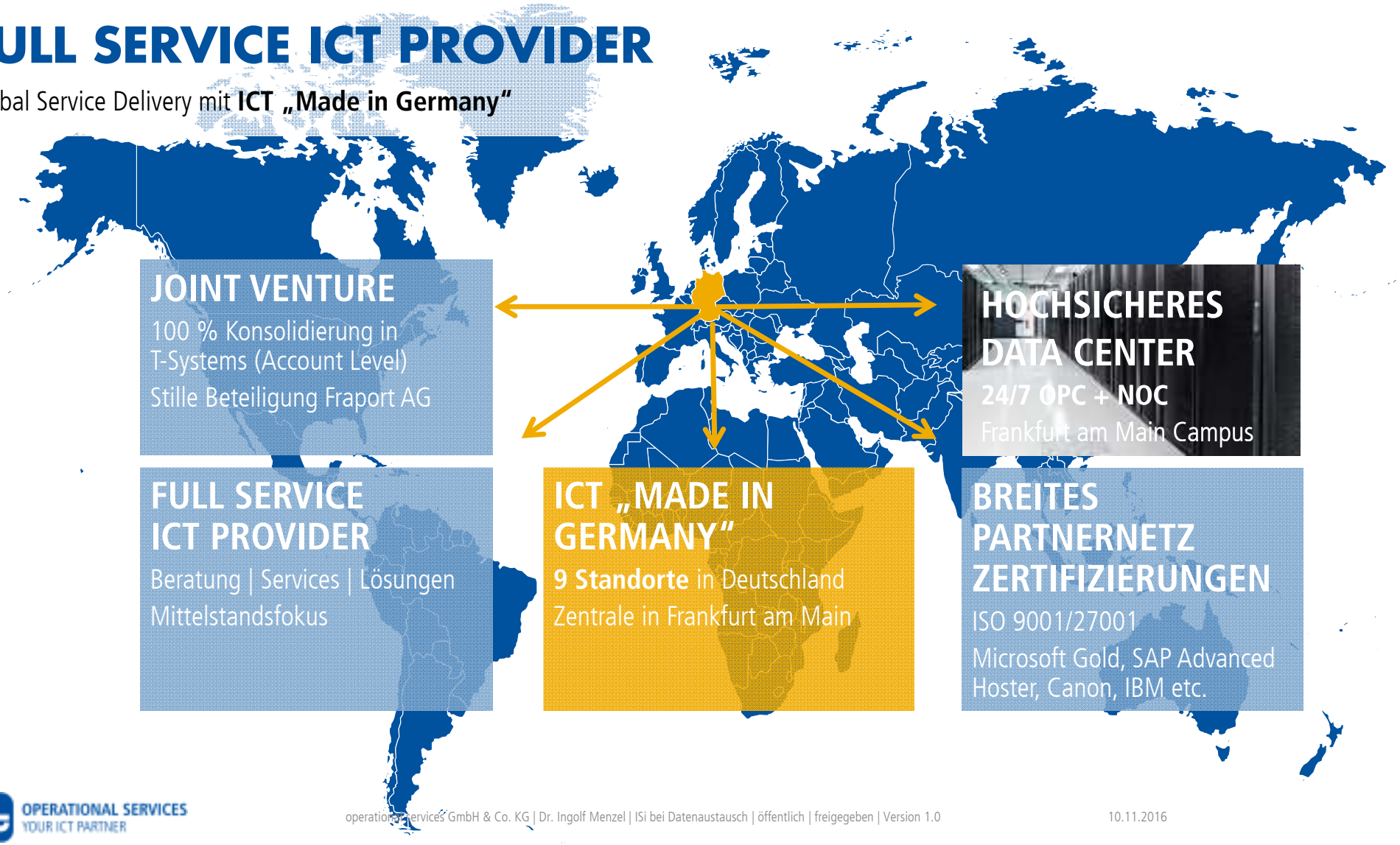
Beijing Auto BJ40L launched on Shanghai Auto Show

INHALT

INHALTLICHE EINORDNUNG IM UNTERNEHMEN OPERATIONAL SERVICES

FULL SERVICE ICT PROVIDER

Global Service Delivery mit **ICT „Made in Germany“**



JOINT VENTURE

100 % Konsolidierung in T-Systems (Account Level)

Stille Beteiligung Fraport AG

HOCHSICHERES DATA CENTER

24/7 OPC + NOC

Frankfurt am Main Campus

FULL SERVICE ICT PROVIDER

Beratung | Services | Lösungen

Mittelstandsfokus

ICT „MADE IN GERMANY“

9 Standorte in Deutschland

Zentrale in Frankfurt am Main

BREITES PARTNERNETZ ZERTIFIZIERUNGEN

ISO 9001/27001

Microsoft Gold, SAP Advanced Hoster, Canon, IBM etc.

FULL SERVICE ICT-LEISTUNGEN

Von der Beratung über Services bis zu vorkonfigurierten Lösungen

SECURITY

Organisation, Applikation und Infrastruktur

↗ **Organisationssicherheit**

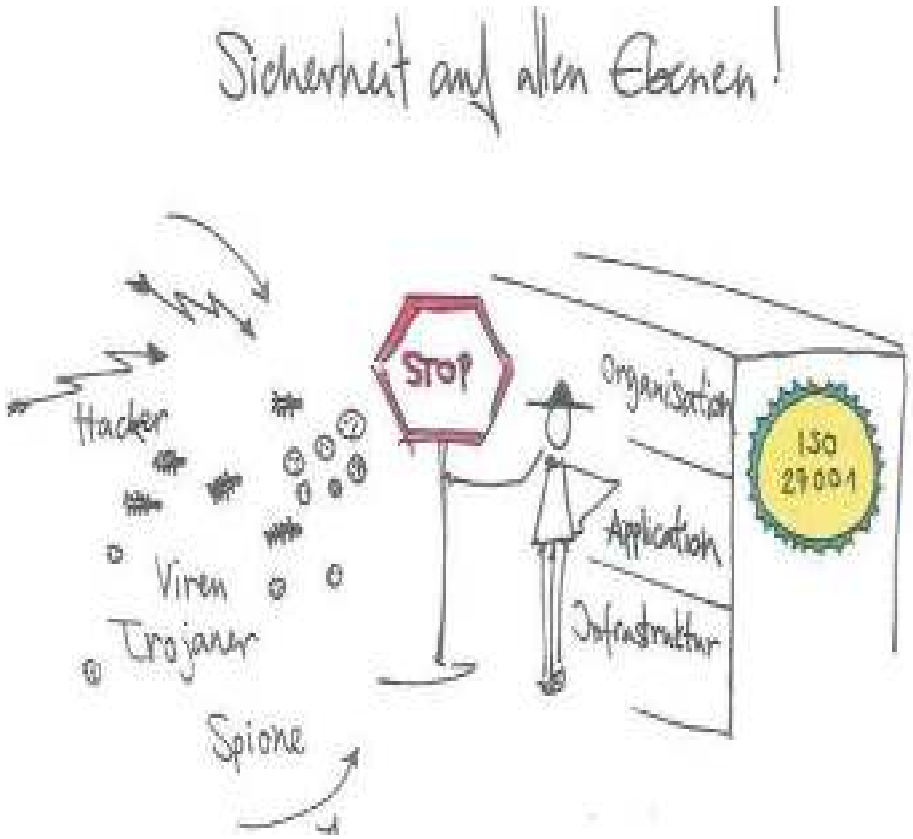
- Sicherheits-Audits
- Anforderungen aus Normen (27001) und gesetzliche Vorgaben:
  Beratung zur Zertifizierung

↗ **Applikationssicherheit**

- Sicherheit in Applikationen durch Codereviews, Design-Guides

↗ **Infrastruktursicherheit**

- Sicherheits-Architektur der Infrastruktur (Schnittstellen, Zonen, Firewalls, etc.)
- Serverhärtung: Absicherung der Daten vor Diebstahl oder Verlust durch Hacker, Trojaner und Viren
- Konfiguration von Sicherheitssoftware (z.B. EPO McAfee)



↗ **Kompetenzen**

- Sicherheitsexperten mit Zertifikaten
- ISO 27001 Lead Auditoren
- TISP/CISSP
- McAfee, G Data

DAS PROZESSMODELL ZUR BEWERTUNG DER INFORMATIONSSICHERHEIT

BEWERTUNG DER INFORMATIONSSICHERHEIT

Motivation des Auftraggebers

1. SICHERSTELLUNG DER INFORMATIONSSICHERHEIT BEI DEN PARTNERN

- Alle notwendigen Prozesse und Anforderungen sind **umgesetzt**.

2. DURCHFÜHRUNG EINHEITLICHER BEWERTUNGEN

- **Einheitliche** Bewertungsverfahren (VDA – Fragebogen)

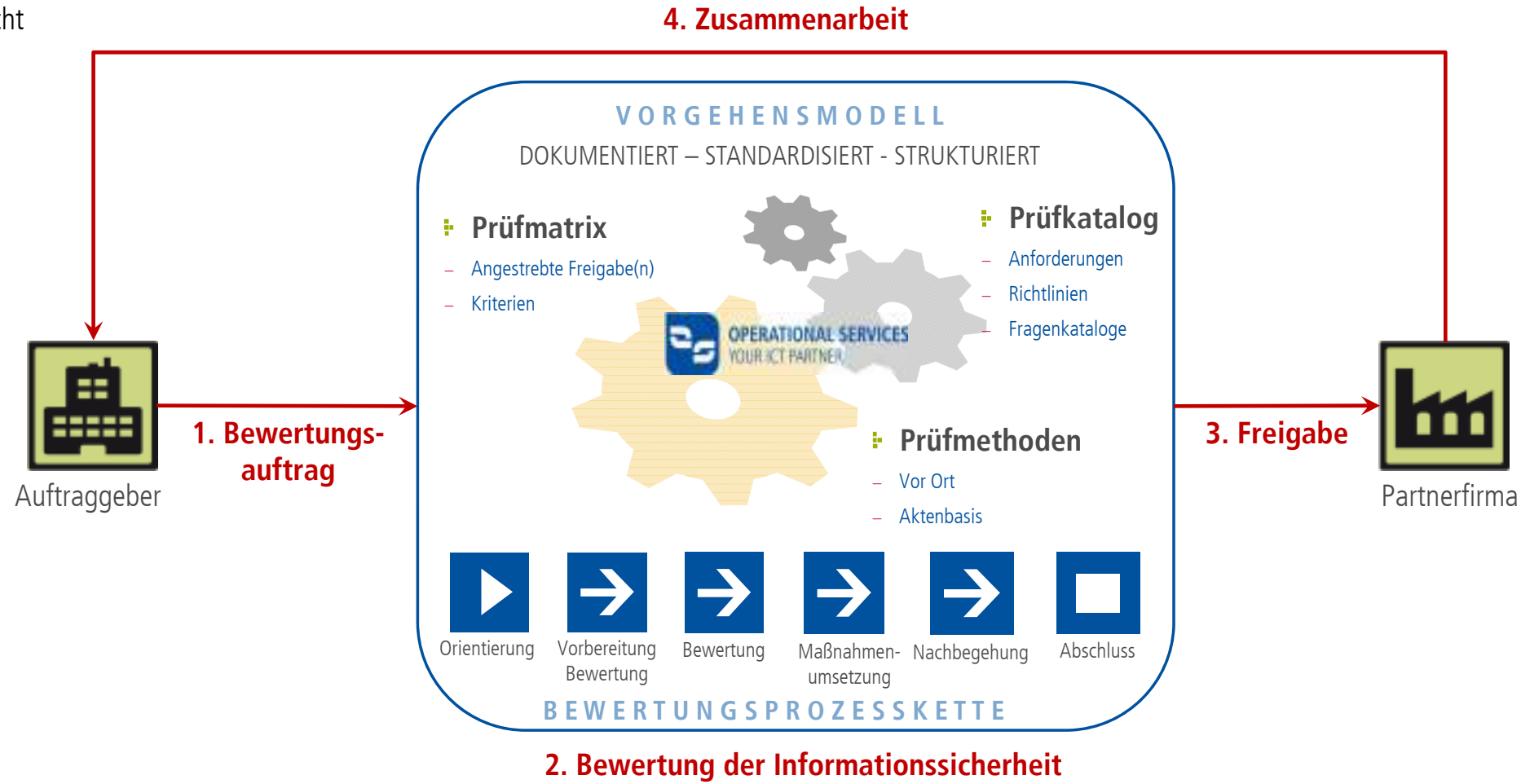
3. UNTERSTÜTZUNG DURCH OS IM PRÜFPROZESS

- **Erläuterung** der Anforderungen
- **Bewertung** existierender IS Prozesse bei der Partnerfirma
- Definition von **Maßnahmen** zur Erhöhung der Informationssicherheit
- **Überwachung** der Umsetzung

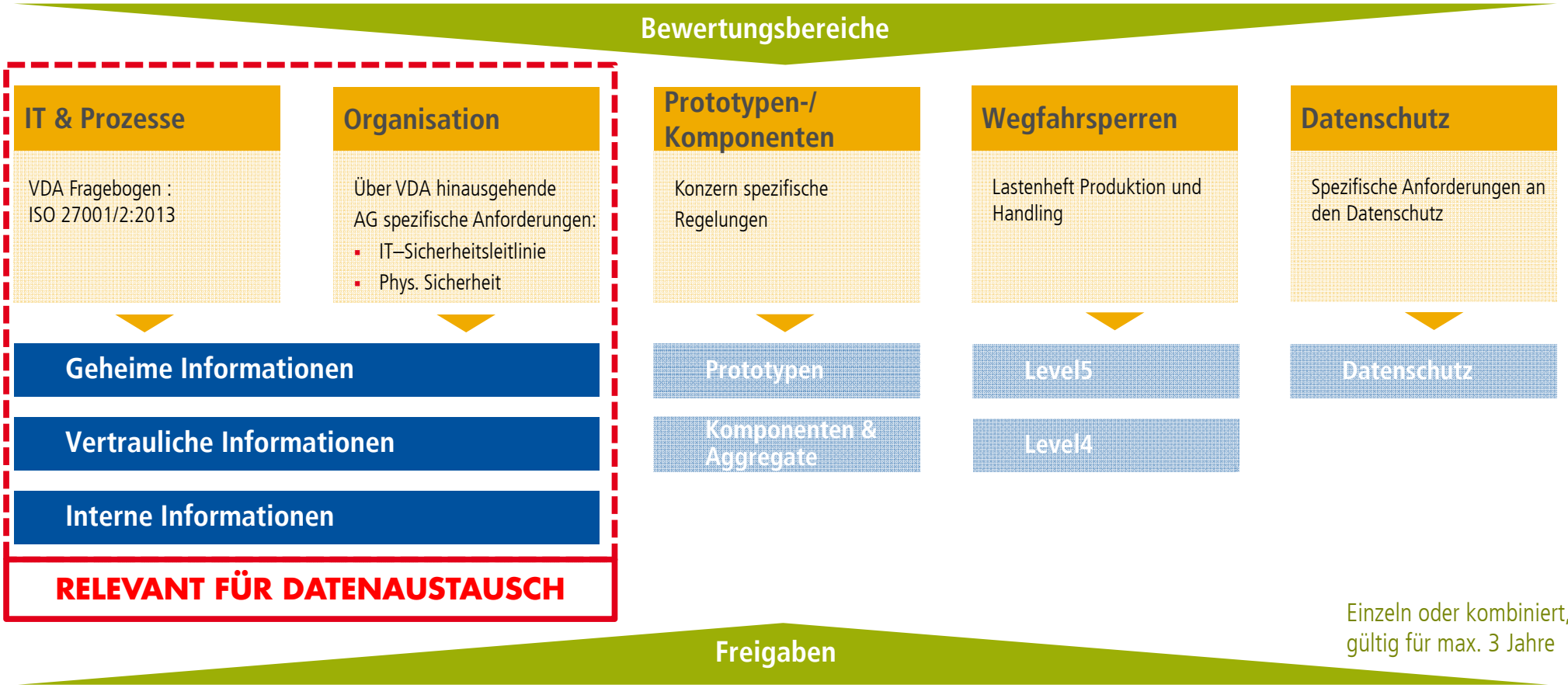
Ziel des Auftraggebers:
AUSSCHLIESSLICHE KOOPERATION MIT PARTNERFIRMEN, DIE EINE ANGEMESSENE INFORMATIONSSICHERHEIT **NACHWEISEN** KÖNNEN.

SERVICE MODELL

Übersicht



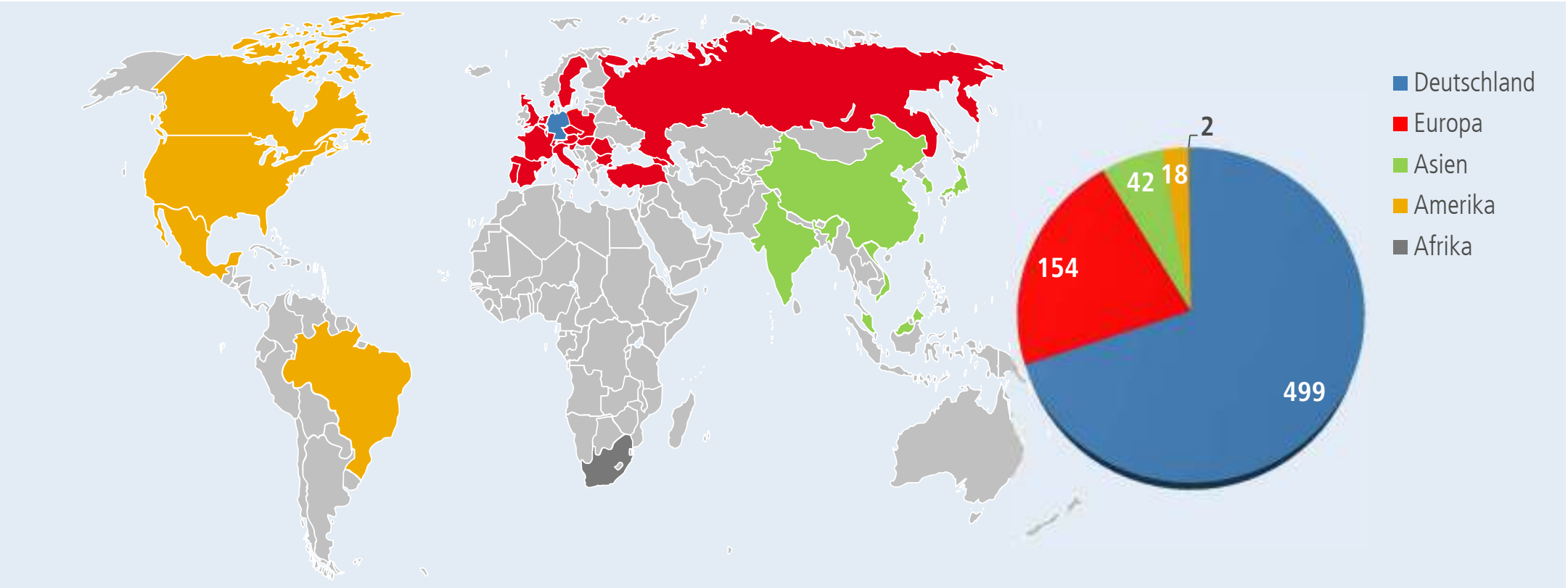
INHALTE DER BEWERTUNG



Einzeln oder kombiniert, gültig für max. 3 Jahre

INSGESAMT 715 BEWERTUNGEN IM JAHR 2015

Anzahl durchgeführter Bewertungen



NUTZEN FÜR PARTNERFIRMEN

PARTNERFIRMEN-INTERNER NUTZEN

- Mitarbeiter machen sich vertraut mit Informationssicherheit, Schaffung von **Bewusstsein**
- Verbesserung der Sicherheit der **eigenen Geschäftsinformationen**
- Verbesserung des übergreifenden Informationssicherheits-Managementsystem – **ein Schritt in Richtung Zertifizierung nach ISO 27001**

WIRKSAMKEIT NACH AUßEN

- Nachweis eines bestandenen VDA-Assessments (VDA Bogen ist bekannt im gesamten Verband der Automobilbauer)
- **Imageverbesserung** in Bezug auf die Informationssicherheit als Volkswagen Partnerfirma

„SICHERHEIT IST NUR SO STARK WIE DAS SCHWÄCHSTE GLIED IN DER KETTE“

ÜBERSICHT DER ANFORDERUNGEN

VERANKERUNG DER PRÜFINHALTE

Branchen- und OEM spezifische Vorgaben (Prüfanforderungen)

- **VDA: I**nformation **S**ecurity **A**ssessment **VDA ISA** (basierend auf ISO 27001)
- Auftraggeber-spezifische **IT Sicherheitshandlungsleitlinien** für Partnerfirmen
- Auftraggeber-spezifische Leitfäden: **Authentifizierung und Verschlüsselung; Datenaustausch**

RELEVANT FÜR DATENAUSTAUSCH

- Richtlinien für **Prototypen** / Transport von Prototypen
- Richtlinie: Produktion und Handling **wegfahrsperren-relevanter Bauteile**
- Anforderungen für **Joint Ventures und Projekthäuser**
- Prozess und Anforderungen für **Arbeitsplatz-Verlagerungen**

1. GRUNDLAGE: VDA ISA

Das VDA - **I**nformation **S**ecurity **A**ssessment

- Fragenkatalog „**Information Security Assessment**“ (Aktuelle Version 2.1.3 (22.05.2015))
- Basierend auf der **ISO 27002:2013**
- **18 Themenkomplexe** / 47 einzelne Controls
- Link: https://www.vda.de/de/services/Publikationen/information-security-assessment.html
- **Reifegrade**: Jede Frage bewertet nach SPICE ISO 15504 **- Level 0-5**

0 → **Unvollständig** (Prozess ist nicht implementiert …)
1 → **Durchgeführt** (Prozesszweck wird erreicht, incl. Arbeitsergebnisse, gesteuert)
2 → **Gesteuert** (Definierte und überwachte Ergebnisse, Schnittstellen incl. Dokumentation)
3 → **Etabliert** (Unternehmens-einheitlicher Standard-Prozess)
4 → **Vorhersehbar** (KPI und Korrekturmaßnahme)
5 → **Optimierend** (Prozessverbesserung, Projekte zur Optimierung)

- **Sinnvolle Vorgabe**: Gesamt - **Zielreifegrad 3,0**

VDA ISA – BEISPIEL: CONTROL 13.4

In wie weit werden Schutzmaßnahmen getroffen, wenn **Informationen ausgetauscht oder übermittelt** werden?

Hierzu gehört u.a.:

+ **Ermittlung der verwendeten Dienste** zur Übertragung
  - wie z.B. E-Mail
  - …

+ **Erstellung von Regeln und Verfahren** gemäß den Vorgaben der Informations**klassifikation** unter Beachtung folgender Punkte:
  - Schutz der Nachrichten vor unberechtigtem Zugriff
  - …

+ **Durchführung** von elektronischem Datenaustausch**, je nach Vertraulichkeitsstufe**, durch verschlüsselte Objekte (z.B. E-Mail, E-Mail Anhänge (PGP, S/Mime)) und / oder mit verschlüsselten Medien statt (z.B. ENX, VPN, verschlüsselte WAN-Verbindungen (HTTPS, SFTP, TLS)).

2. GRUNDLAGE: LEITFADEN DATENAUSTAUSCH

In wie weit werden **Schutzmaßnahmen** getroffen, wenn **Informationen ausgetauscht oder übermittelt** werden?

Informationen klassifizieren	• **Datentyp / Vertraulichkeit / Größe**
Empfänger klassifizieren	• **Interner Mitarbeiter / Partnerfirma**
Verfahren auswählen	• **Verfahren nach o.g. Kriterien auswählen**
Freigabe und Protokollierung	• **ggf. Weitergabe nach Zustimmung / elektronisches bzw. manuelles Protokoll**
Verschlüsselung auswählen	• **Tool oder integriertes Verfahren / Passwort auf separatem Kanal**
Austausch starten	• **Weiterführende Informationen im Detail beachten**

3. ASPEKT: ROUTING VON DATEN

Tatsächliche Situation

- Daten-Zugänge von Auftraggebern
  könnten **über LAN/WAN-Verbindungen**
  Dritten bereitgestellt werden (Routing).

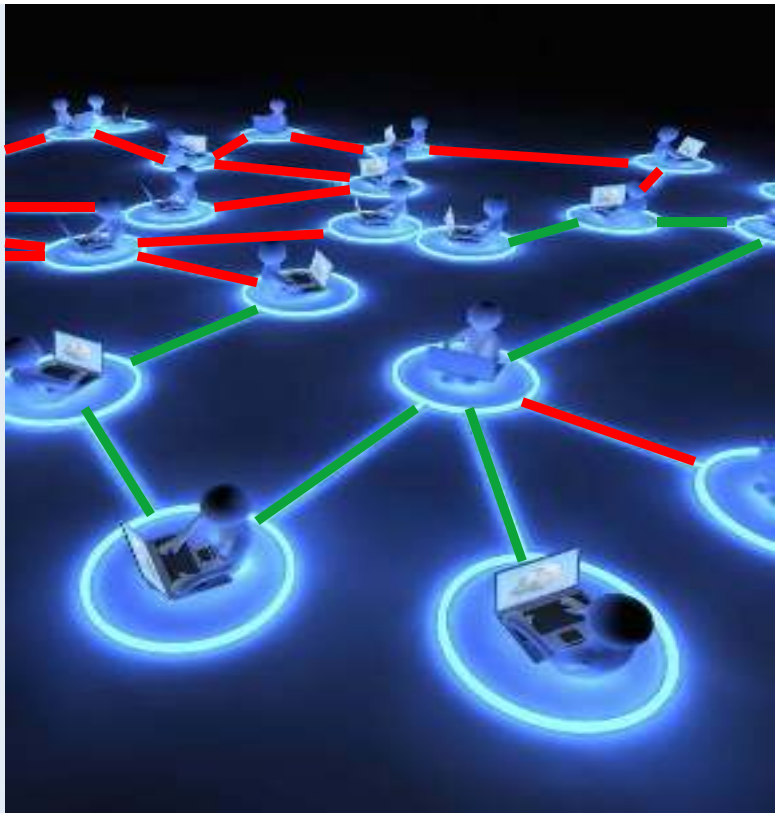
- **Keine** technische Möglichkeit
  zur **Beschränkung** oder Überwachung.

3. ROUTING VON DATEN

- Die netztechnische Weiterleitung (Routing) ist nur gestattet,
  wenn das Routing ausschließlich **innerhalb des Netzes der Partnerfirma** und
  ausschließlich **über und zu Firmenstandorten** der Partnerfirma erfolgt,
  die eine Freigabe besitzen.

- Die Freigabe muss dabei mindestens der **erforderlichen Vertraulichkeitsklasse**
  (intern/vertraulich/geheim) der auszutauschenden Informationen entsprechen.

- Die **Verbindungen** zu weiteren Firmenstandorten der Partnerfirma
  müssen durch die Partnerfirma **verschlüsselt** werden.



PRAXISBEISPIELE AUS DEM AUDITALLTAG

FAZIT NACH 5 JAHREN

Häufige Situation in den Firmen

Kleine Firmen

Es fehlen immer noch Basics, besonders im Ausland („es ist noch nie etwas passiert…").

Mittlere Firmen

profitieren von anderen bereits auditierten Standorten.

Große Unternehmen

Interne Audits durchlaufen, bevor wir kommen (übergreifende Regeln sind ausgerollt).

Physische Sicherheit

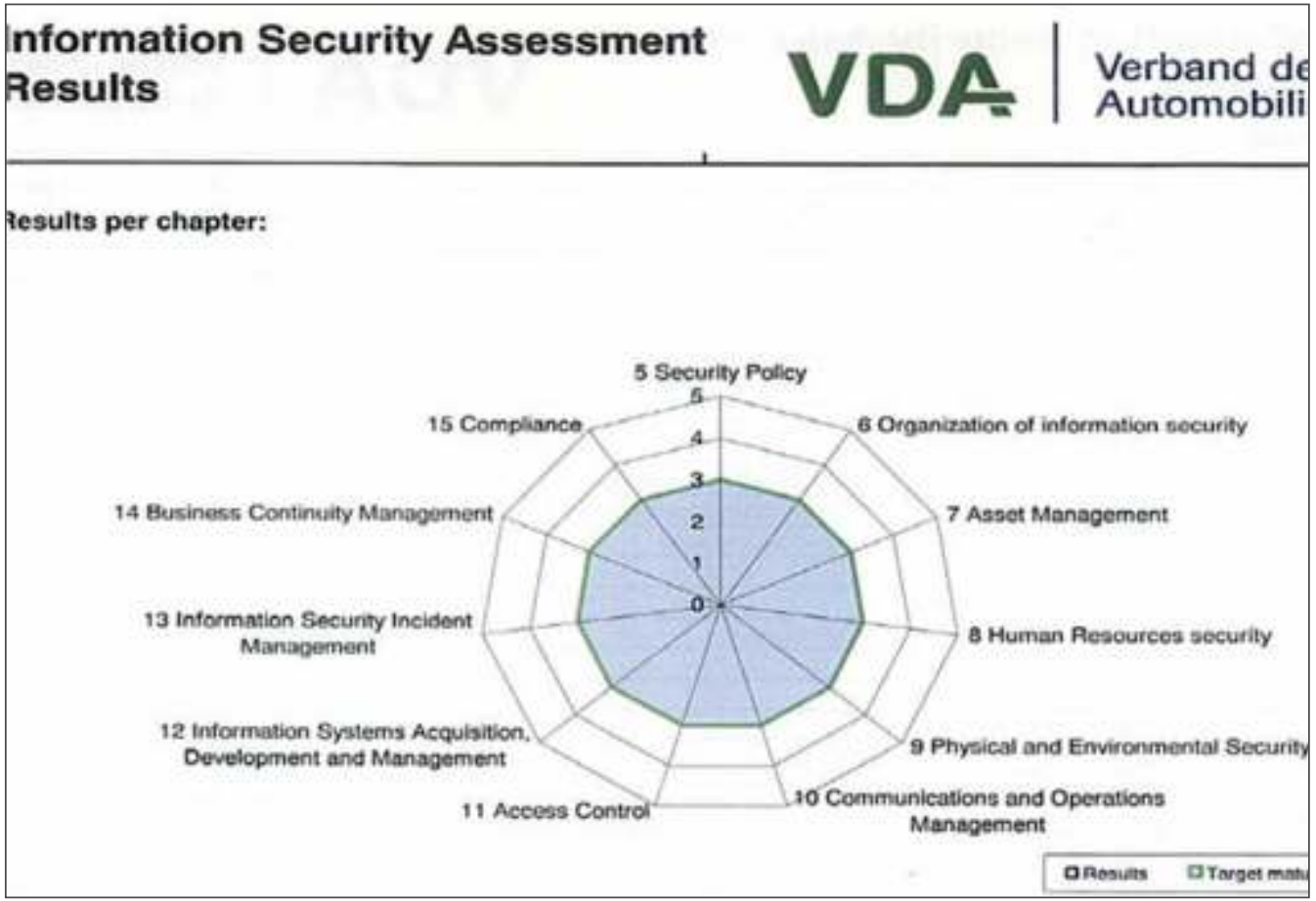
wird häufig nicht als Gesamtkonzept umgesetzt → „Hintereingänge" stehen offen.

Starke Authentifizierung und verschlüsselte Speicherung

ist fast nie vorhanden, da die Anforderung meist nicht bekannt ist (für sensible Daten).

RÜCKLÄUFER: SELBSTAUSKUNFT VDA ISA

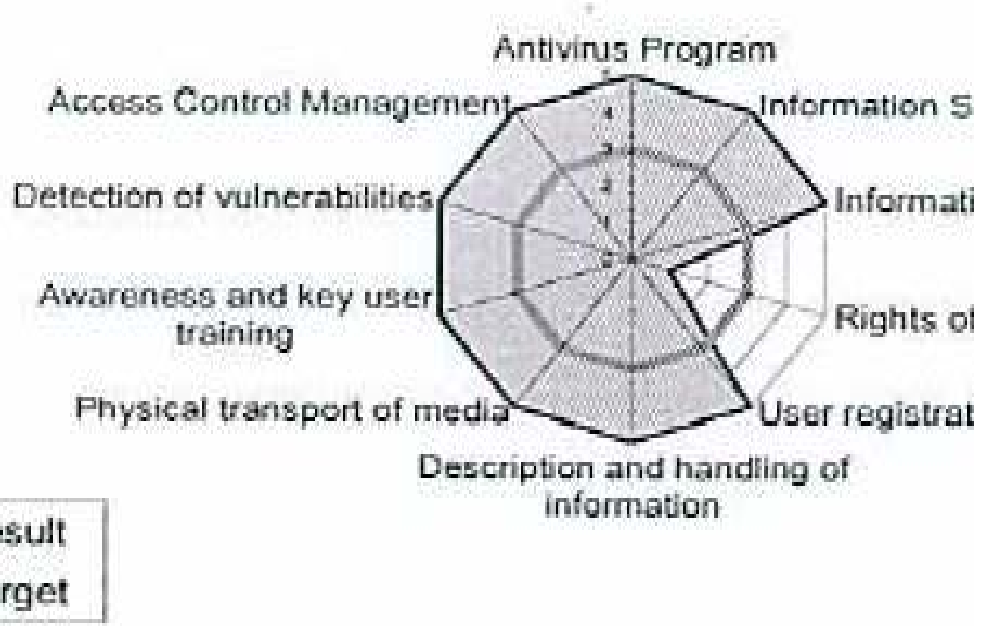
Alte Version: Rückantwort 1 = 100%



RÜCKLÄUFER: SELBSTAUSKUNFT VDA ISA

Alte Version: Rückantwort 2

Result	Target
5	3
5	3
5	3
1	3
5	3
5	3
5	3
5	3
5	3
5	3



BEGEHUNG

Bequemlichkeit…

… und Erfindergeist

BEGEHUNG

Raucherausgang

PHYSISCHE SICHERHEIT

Vor Ort im…

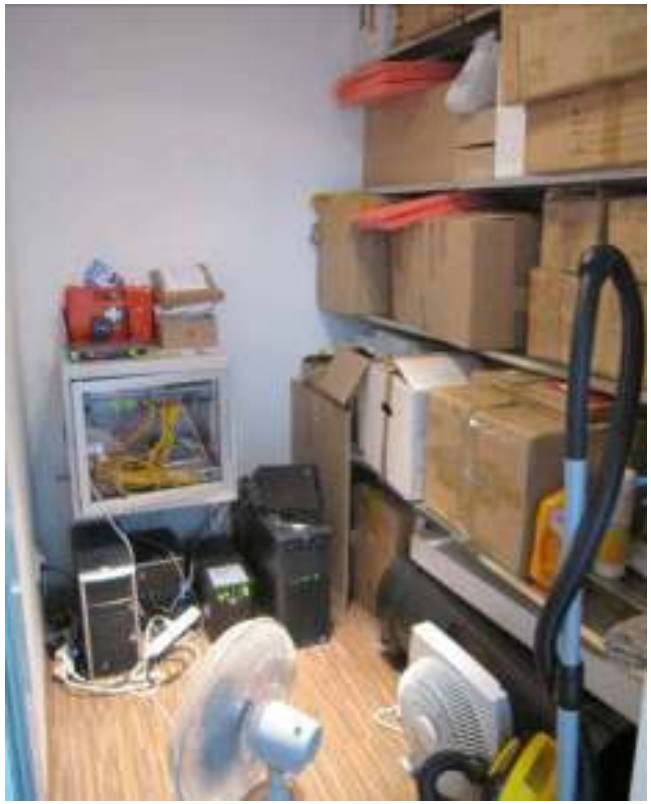
… Serverraum

PHYSISCHE SICHERHEIT

Confidentiality and Availability!

BRANDLASTEN

Weitere Serverräume



SICHERE KOMMUNIKATION ?

Übermittlung von Nachweisen

Betreff: [redacted] implementation following to Assessment Report
Wichtigkeit: Hoch

M. Menzel,

I'm pleased to inform you that we just have finished all the 27 implementation needed and wanted to be certificated.
All the answers are waiting you in our SFTP.

To access to the folder on SFTP : (only with a software like FileZilla, not with your Internet Navigator)
ftp[redacted]com
User : [redacted]_VW_AUDITEUR
Password : 01N5JB2t

To open the encrypted zip :
Password : iucAC1HR

MEHRWERTE SCHAFFEN

OS UNTERSTÜTZT VIELFÄLTIG

- **Informationssicherheit**
  - **Quick-Check:** Informationen, Orientierung und Statusbestimmung
  - **Vorbereitung auf Zertifizierung** ISO 27001 / ISO 9001
    - **Gap-Analysen**
    - **Coaching**
  - **Optimierung** des Integriertes Managementsystem (**IMS**)
  - **Trainings** für Informationssicherheit / Awareness
  - Erarbeitung von **Dokumentationen**
  - Reviews, interne **Audits**
  - Extern bestellter **Informationssicherheits-Beauftragter** (CISO) und **Datenschutz-Beauftragter**

OS UNTERSTÜTZT VIELFÄLTIG

- **Lieferanten-Audits im Automobil-Sektor**
  - **Vorbereitung** auf die Bewertung
  - **Nachbereitung**
    Unterstützung bei der Umsetzung von Maßnahmen nach einem Audit

- **IT Sicherheit**
  - **Fachlicher Support**
    - Verschlüsselung, PKI,
    - Netzwerke, Penetration Tests
    - Applikations-Sicherheit
  - **Systemanalysen**

SICHERE KOMMUNIKATION !

Übermittlung von Nachweisen

An: Menzel, Ingolf
Betreff: [WARNING: MESSAGE ENCRYPTED]Evaluation of Information Security

Guten Tag Herr Menzel,

Anbei finden Sie bitte die angeforderten Informationen.
Das pwd für die Zip Dateien wird per SMS gesendet.

Mit freundlichen Grüssen,

VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT!

www.operational-services.de

SERVICES

LÖSUNGEN

BERATUNG

Sven Wollrabe
Projektleiter
Telefon: +49 151 12643617
E-Mail: Sven.Wollrabe@o-s.de

Dr. Ingolf Menzel
ISO 27001 Lead Auditor
Telefon: +49 172 3488295
E-Mail: Ingolf.Menzel@o-s.de