TISAX-Prüfungen in der Automobilindustrie

Vortrag zur Informationssicherheit in der Lieferkette

IT-SECURITY @ WORK

UIMC®

Agenda

- Ausgangssituation
- Was ist TISAX / Was sind die Ziele von TISAX?
- Prüfprozess mit Darstellung der Rolle Externer
- Säulen / Charakterisieren des Verfahrens
- Erfahrung aus der Praxis
- Was ist nötig um sowas durchzusetzen?

Referent I
Marion Steiner

- Dipl. Inform. TU Darmstadt
- Senior Consultant bei der IT-Security@Work GmbH (ISW)
- Tätigkeitschwerpunkte
  - Informationssicherheit und Datenschutz
- Externer DSB / ISB
- Begleitung Kunden bei TISAX-, KRITIS- oder ISO27001-Prüfungen
- Ehem. Auditor PCI DSS / PA DSS
- Mitglied des Leitungsgremiums der Fachgruppe Security Management bei der Gesellschaft für Informatik (GI)

Referent II
Benedict Voßbein

- M. Sc. in Wirtschaftsinformatik an der Universität Duisburg Essen
- Studienschwerpunkte; (u. a. IT-Management)
- Seit 2017 als Berater bei der UIMC
- Tätigkeitschwerpunkte
  - Informationssicherheit
  - und Datenschutz
- IRCA Lead Auditoren Zertifizierung nach ISO 27001
- Mitglied des Leitungsgremiums der Fachgruppe Security Management bei der Gesellschaft für Informatik (GI)

Ausgangsituation

- Zunehmender Bedeutungsgewinn von Informationen und Informationssystemen und deren Verarbeitung in allen Branchen.
- Mit Möglichkeiten und Chancen gehen immer auch Risiken einher
- Der Verband der Automobilindustrie (VDA) entwickelt in dem Arbeitskreis Informationssicherheit Standards zur Wahrung der Informationssicherheit und des Prototypenschutzes

Problem der OEM: Angriff über Zulieferer

Ausgangsituation

- Betroffen sind alle Lieferanten oder Dienstleister
- Umsetzung zunächst via ISO 27001 + Prototypenschutz
- Entwicklung des VDA ISA (Information Security Assessment)
  - Eigener Fragenkatalog auf Basis ISO 27001
  - Ebenfalls Informationssicherheit + Prototypenschutz

Was ist TISAX / Was sind die Ziele von TISAX?

Was ist TISAX?

- Trusted Information Security Assessment Exchange (TISAX)
- „TISAX ist ein Prüf- und Austauschmechanismus [der ENX] für die Informationssicherheit von Unternehmen [in der Automobilbranche] und ermöglicht eine gemeinsame Anerkennung von Prüfergebnissen zwischen den Teilnehmern“
- ENX Association ist ein Zusammenschluss von Automobilherstellern, Zulieferern und vier nationalen Automobilverbänden

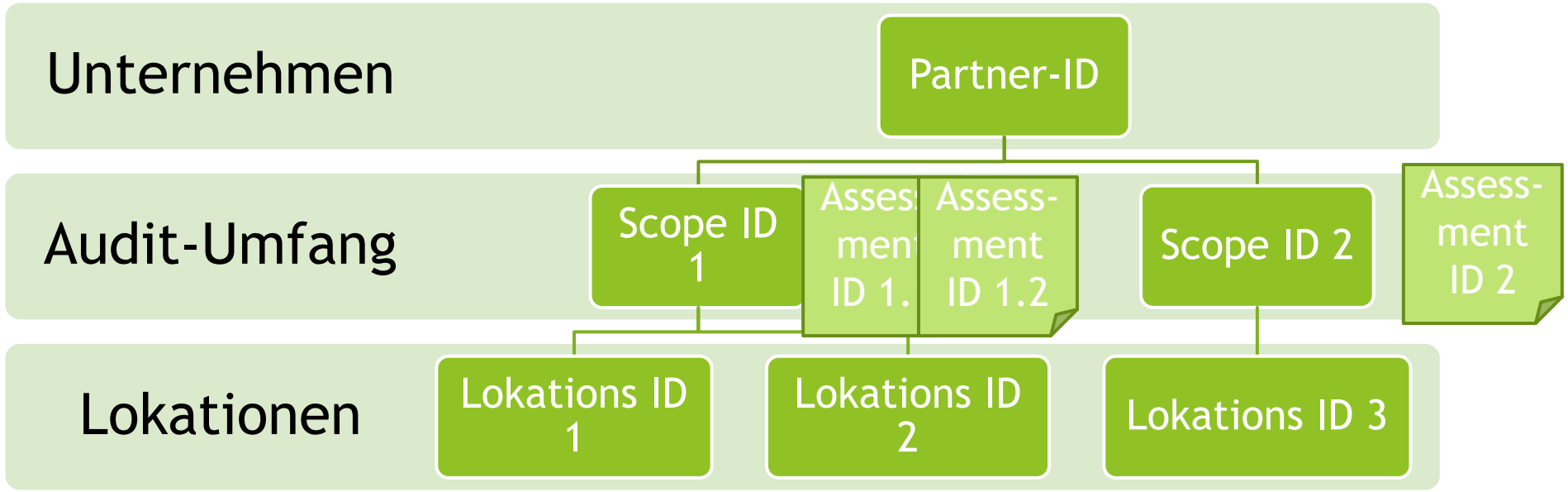
Was sind die Ziele von TISAX?

- Standardisierte Prüfung durch einheitlichen Fragenkatalog
- Einheitliche Genehmigung von Prüfdienstleistern durch ENX
- Standardisierte Prüfergebnisse
- Austausch von Prüfergebnissen unter den Teilnehmern
- Selbstbestimmung mit welchen Teilnehmern Ergebnisse in welcher Detailtiefe geteilt werden

TISAX - Prozess

Quelle: https://www.enx.com/de-de/tisax/

Referenzierbare Informationen



SHARING LEVEL "A: ASSESSMENT-RELATED INFORMATION" + TISAX LABELS - EXAMPLE

Shared Location A + Labels

Search for...

Export Published & Shared Results as Excel

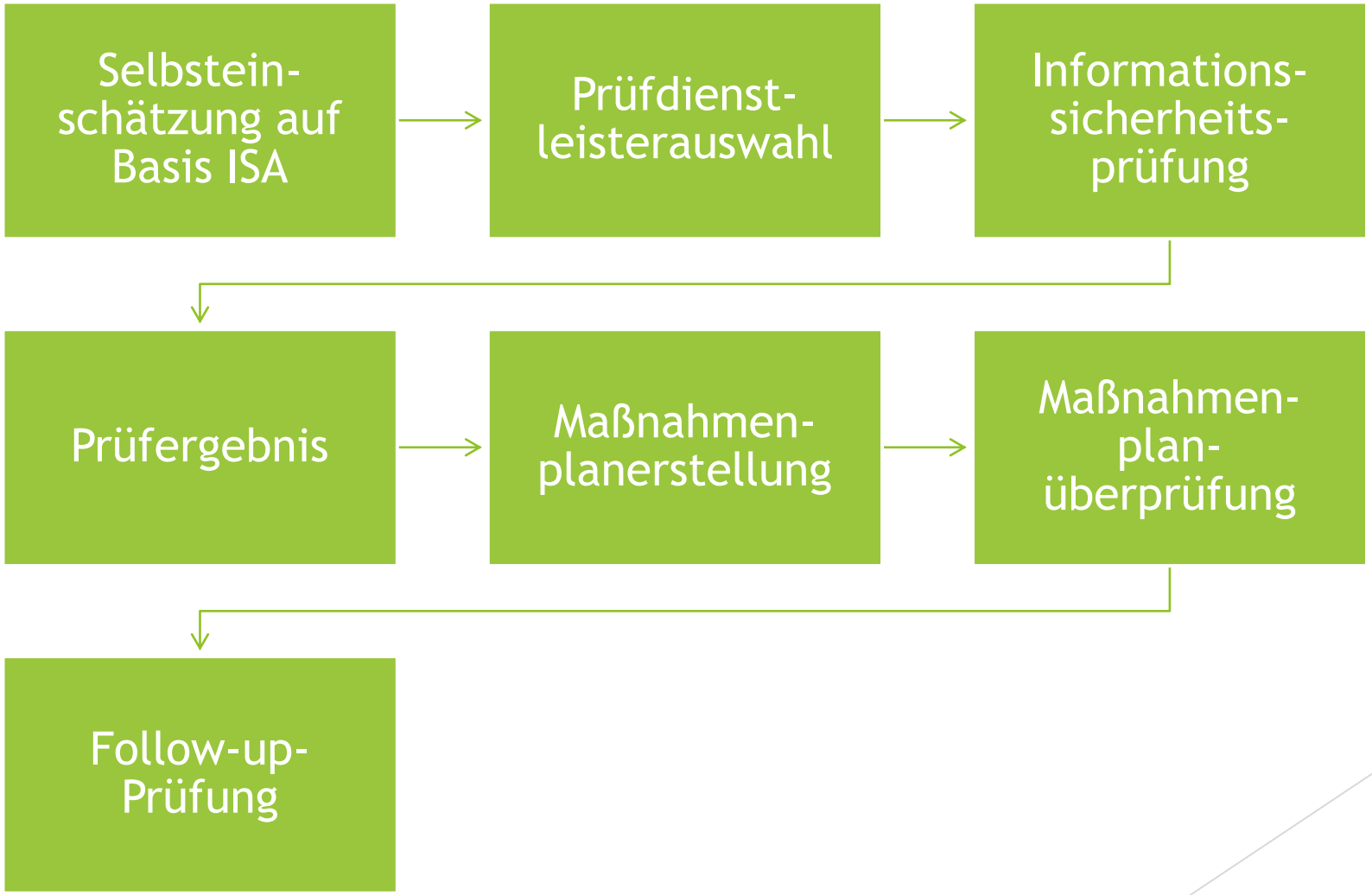
PREVIEW EXAMPLE

Participant	Scope ID	DUNS	Company	Street and No.	Postal Code	City	Country	Assessment	Status	Report Date	TISAX Label	Validity
ENX Association	S00000	312614179	ENX Association	Bockenheimer Landstrasse 97	60325	Frankfurt am Main	Germany	A00000	Finished	1/2/2018	Info High; Info Very High;	1/2/2021

TISAX - Prozess

Quelle: https://www.enx.com/de-de/tisax/

Der Prüfprozess



Die Assessment-Level

Prüfmethode	Assessment-Level 1 (AL 1)	Assessment-Level 2 (AL 2)	Assessment-Level 3 (AL 3)
Prüfung der Selbsteinschätzung	Nur Überprüfung, ob Selbsteinschätzung vorhanden ist	Ja	Ja
Nachweise	Nein	Plausibilitätsprüfung	Eingehende Prüfung
Interviews	Nein	Als Telefonkonferenz.	Persönlich, vor Ort
Vor-Ort-Prüfung	Nein	Auf Ihren Wunsch	Ja

Quelle: https://www.enx.com/de-de/tisax/

Prüfziele / Assessment-Level

Nr.	TISAX-Prüfziel	Assessment Level
1.	Informationen mit hohem Schutzbedarf Information	AL2
2.	Informationen mit sehr hohem Schutzbedarf Information	AL3
3.	Schutz von Prototypen-Bauteilen und -Komponenten	AL3
4.	Schutz von Prototypenfahrzeugen	AL3
5.	Umgang mit Erprobungsfahrzeugen	AL3
6.	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings	AL3
7.	Datenschutz Gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz-Grundverordnung (DSGVO)	AL2
8.	Datenschutz bei besonderen Kategorienpersonenbezogener Daten Gemäß Artikel 28 („Auftragsverarbeiter“) mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben	AL3

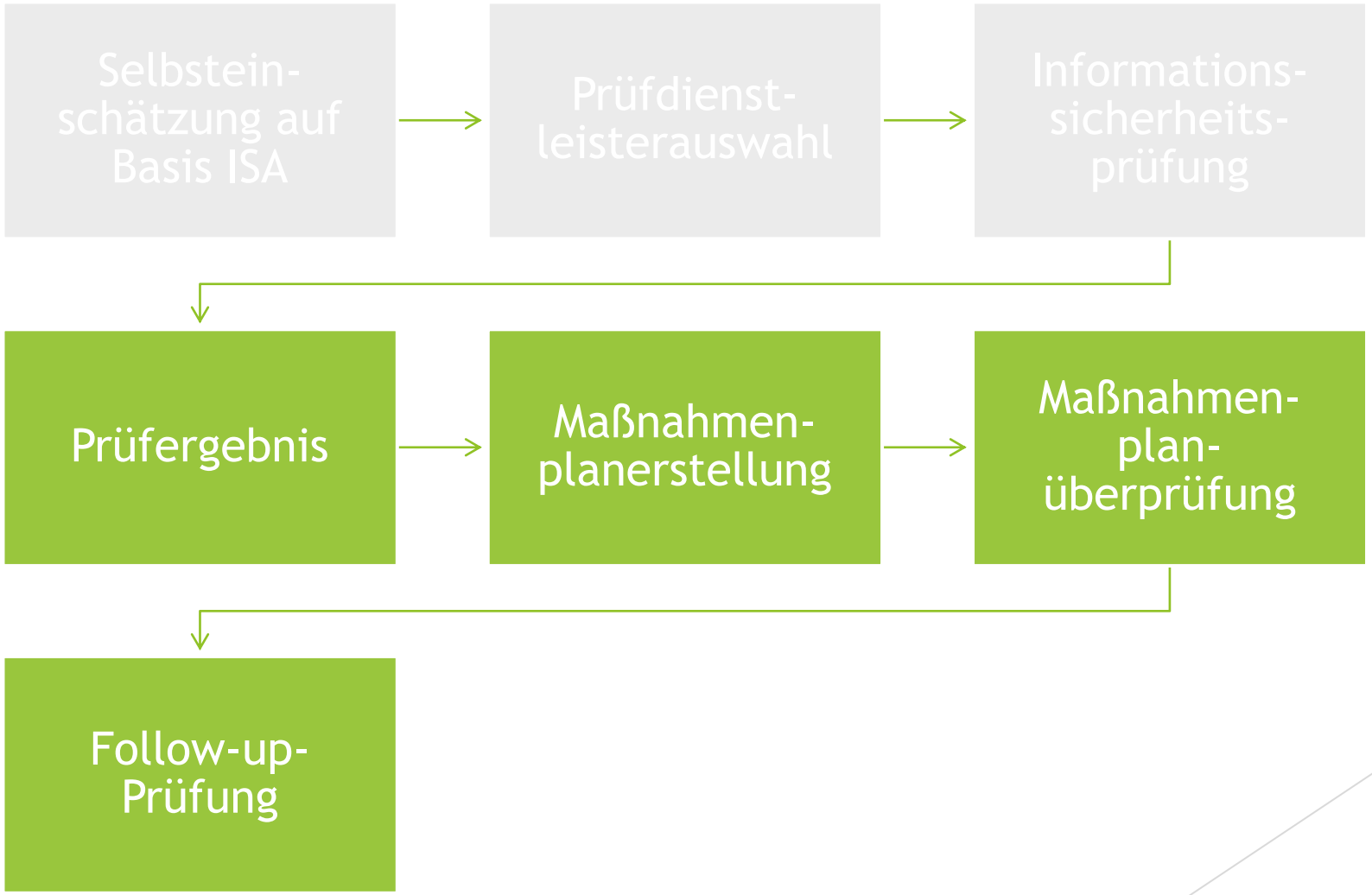
Quelle: https://www.enx.com/de-de/tisax/

Reifegrade

Reifegrad	In einem Wort	Beschreibung
0	**Unvollständig**	Es gibt keinen Prozess, es wird keinem Prozess gefolgt oder der Prozess ist nichtgeeignet das Ziel zu erreichen.
1	**Durchgeführt**	Es wird einem nicht oder unvollständig dokumentierten Prozess gefolgt und es existieren Indizien das er sein Ziel erreicht.
2	**Gesteuert**	Es wird einem Prozess gefolgt, der seine Ziele erreicht. Prozessdokumentation und Prozessdurchführungsnachweise sind vorhanden.
3	**Etabliert**	Es wird einem Standardprozess gefolgt, der in das Gesamtsystem integriert ist. Abhängigkeiten zu anderen Prozessen sind dokumentiert und geeignete Schnittstellen geschaffen. Es existieren Nachweise, dass der Prozess über einen längeren Zeitraum nachhaltig und aktiv genutzt wurde.
4	**Vorhersagbar**	Es wird einem etablierten Prozess gefolgt. Die Wirksamkeit des Prozesses wird durch Erheben von Kennzahlen kontinuierlich überwacht. Es sind Grenzwertedefiniert, bei denen der Prozess als nicht hinreichend wirksam angesehen wird und angepasst werden muss. (Key Performance Indicators)
5	**Optimierend**	Es wird einem vorhersagbaren Prozess gefolgt, bei dem die kontinuierliche Verbesserung wesentliches Ziel ist. Die Verbesserung wird von dedizierten Ressourcen aktiv vorangetrieben.

Quelle: https://www.enx.com/de-de/tisax/

Der Prüfprozess



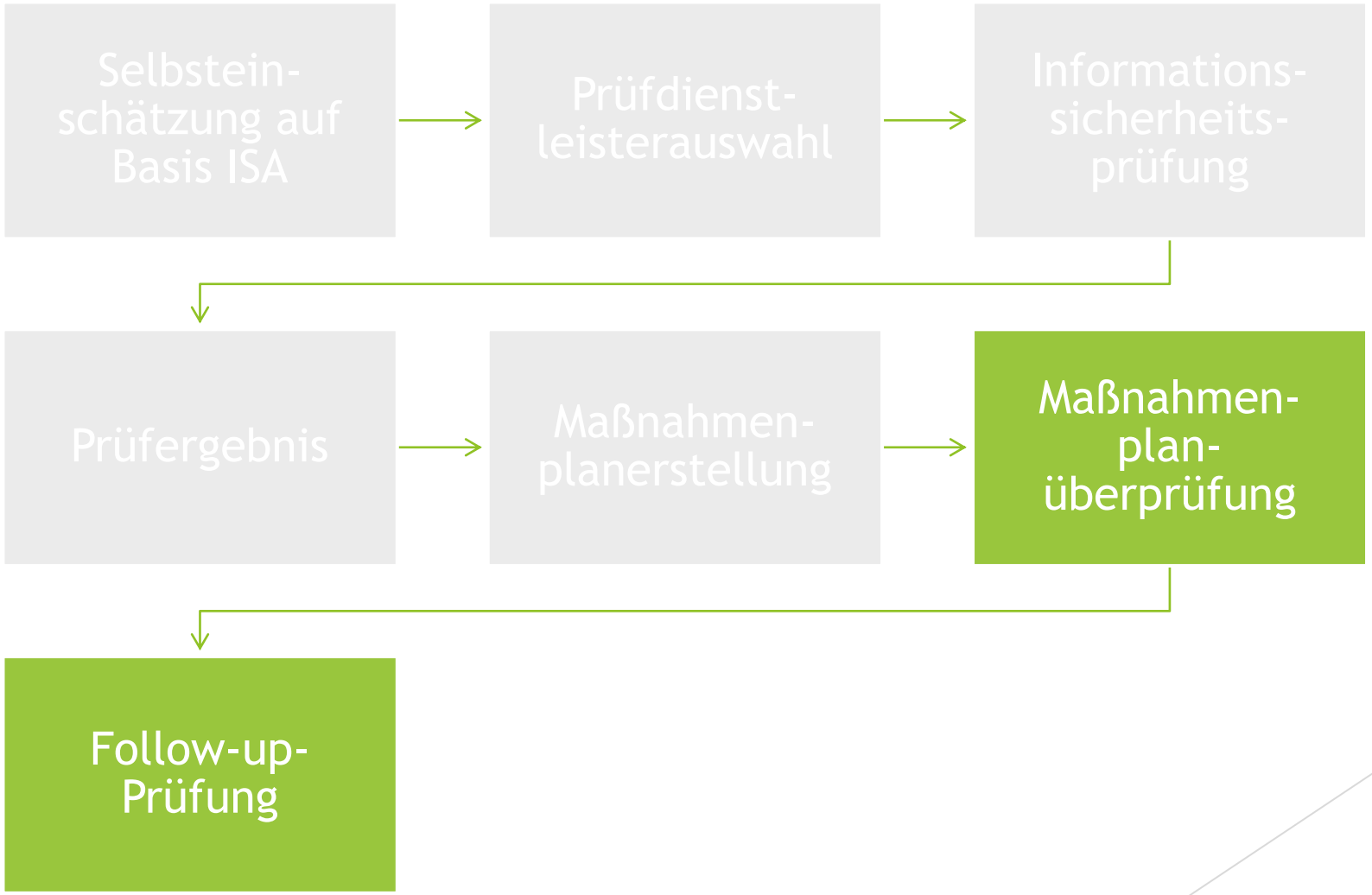
Ergebnisdarstellung

- Konform (≥3,0)
  - oder ≥ 2,7 ohne kritische Abweichungen
- Nebenabweichend (2,7 > 2,1)
  - Es müssen Maßnahmen definiert sein, die zur Beseitigung der Nebenabweichung führen
- Hauptabweichend (< 2,1)
  - Nicht behandelte (Neben)Abweichungen

- Erstellung eines Maßnahmenplans
  - Umsetzungszeitraum
    - 3 Monate (Begründung warum)
    - 6 Monate (Nachweis, dass keine schneller Umsetzung möglich ist)
    - 9 Monate max. Zeitraum für Maßnahmen

Quelle: https://www.enx.com/de-de/tisax/

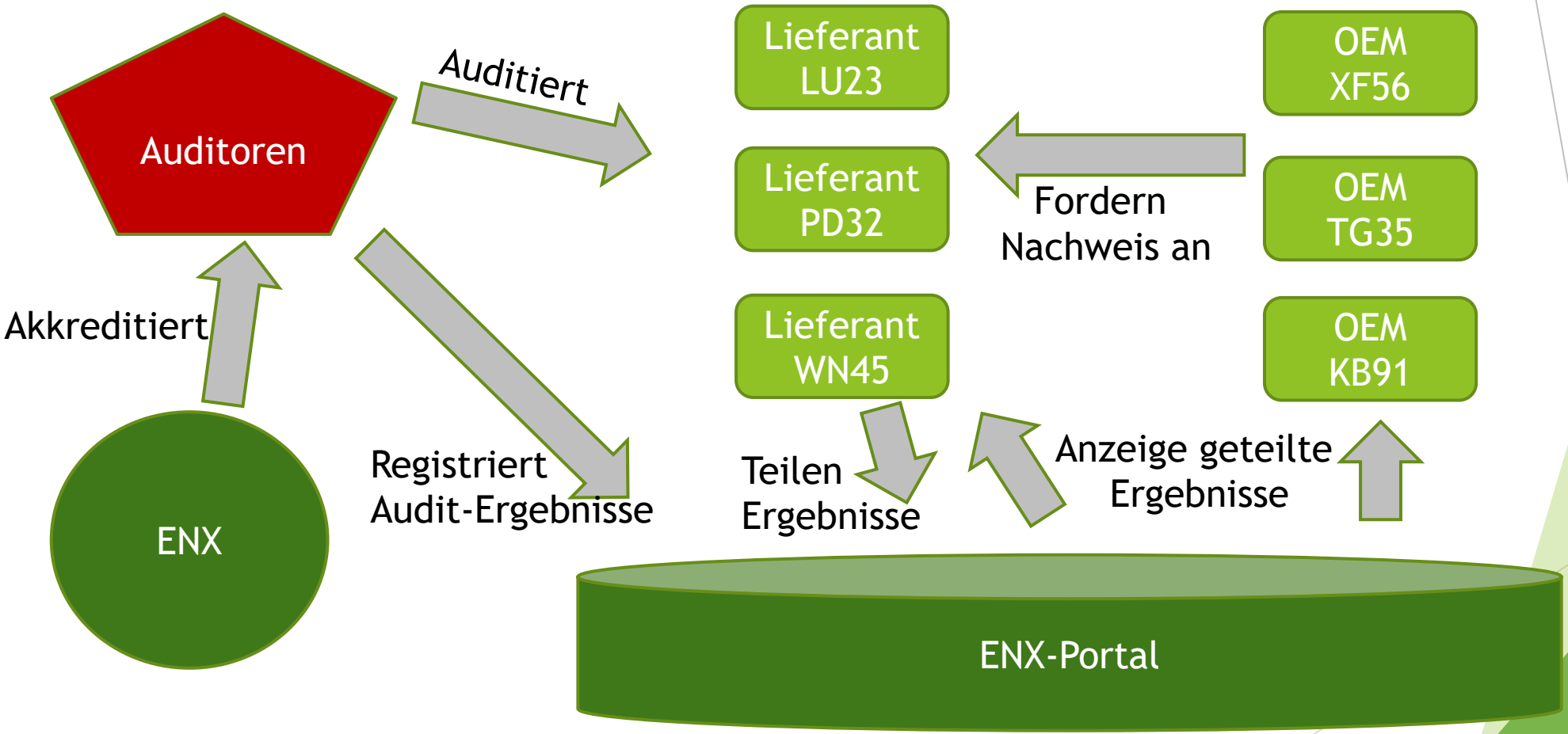
Der Prüfprozess



TISAX - Prozess

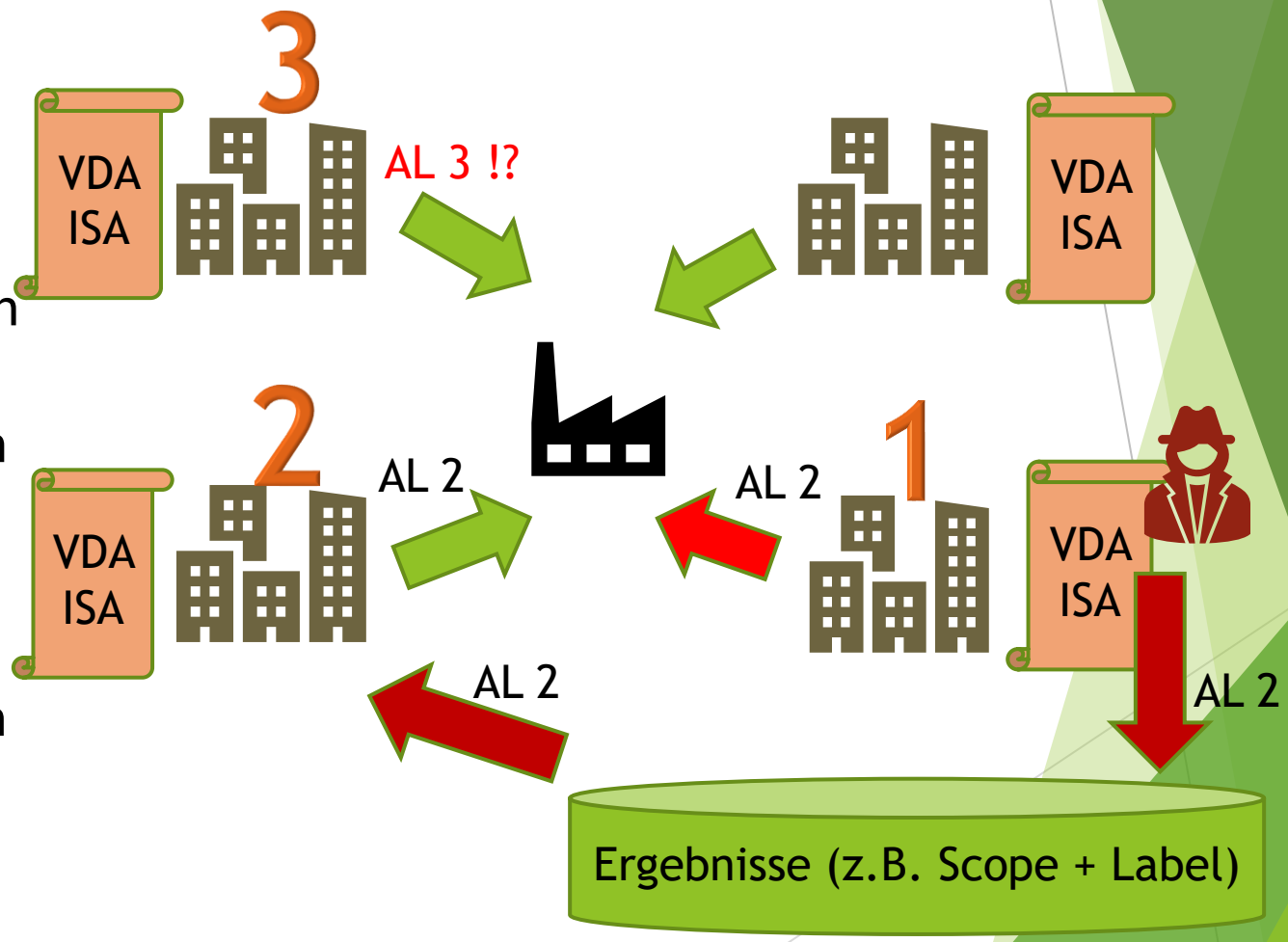
Quelle: https://www.enx.com/de-de/tisax/

Darstellung der Zusammenhänge

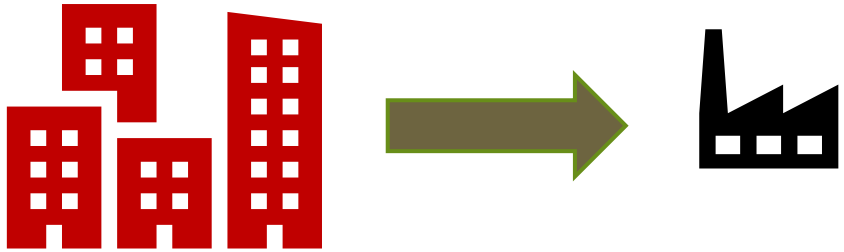


Säulen / Charakterisieren des Verfahrens

- Einheitliche Prüfkataloge/ Prüfschemata
- Von ENX akkreditierte Auditoren -> Fiktion einer vergleichbaren Interpretation von Anforderungen
- „geschlossenes System“, Nachweise haben nur im Rahmen dieser Plattform wirklich Relevanz
- keine „Zertifizierung“
- Tätigkeiten des Zulieferers legen nötiges Anforderungsprofil für Nachweise beim Kunden fest
- ENX-Konsortium ist „zentrale Macht“

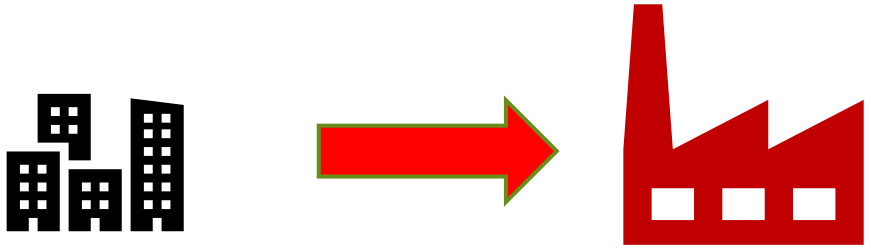


Wann funktioniert das Ganze?



Machtverhältnis relevant:

- Zulieferer ersetzbar, „Bittsteller“
- Auditierung kann erzwungen werden.
- „Nachweis oder keine Beauftragung“



- Zulieferer hat Alleinstellung
- OEM ist auf Ihn angewiesen, „Bittsteller“
- „OEM soll sich doch anderen suchen“ ;-)

Funktioniert das Ganze?

OEM

- Eine einheitliche Bewertung über verschiedene Bauteile hinweg ist nicht immer gegeben
- Eine einheitliche Bewertung unter den OEMs ist nicht zwingend geben
- Unterschiedliche OEMs gehen manchmal „unterschiedliche“ Wege

Auditor

- Bewertung von Maßnahmen ist bei Auditoren nicht zwingend gleich
- Unterschiedliche Qualität der Auditoren entsprechend ihrer Schwerpunkte
- Der Weg zur Erlangung einer „Akkreditierung“ ist eher aufwändig

Dienstleister/ Zulieferer

- TISAX / Informationssicherheit wird eher als Last wahrgenommen
- Der Druck der OEMs zwingt die Dienstleister in der Regel
- Häufig aus der zweiten Sicht erst ein Gewinn

Wie geht es weiter?

- Abbildung der Organisationsstrukturen wird ausgebaut
- Stärkere Verpflichtung der Zulieferer – mehr OEM schließen Zulieferer ohne Nachweis aus
- Stärkere Internationalisierung der Nachweispflichten

Fragen??

Mancher ertrinkt lieber,
als daß er um Hilfe ruft.

– Wilhelm Busch