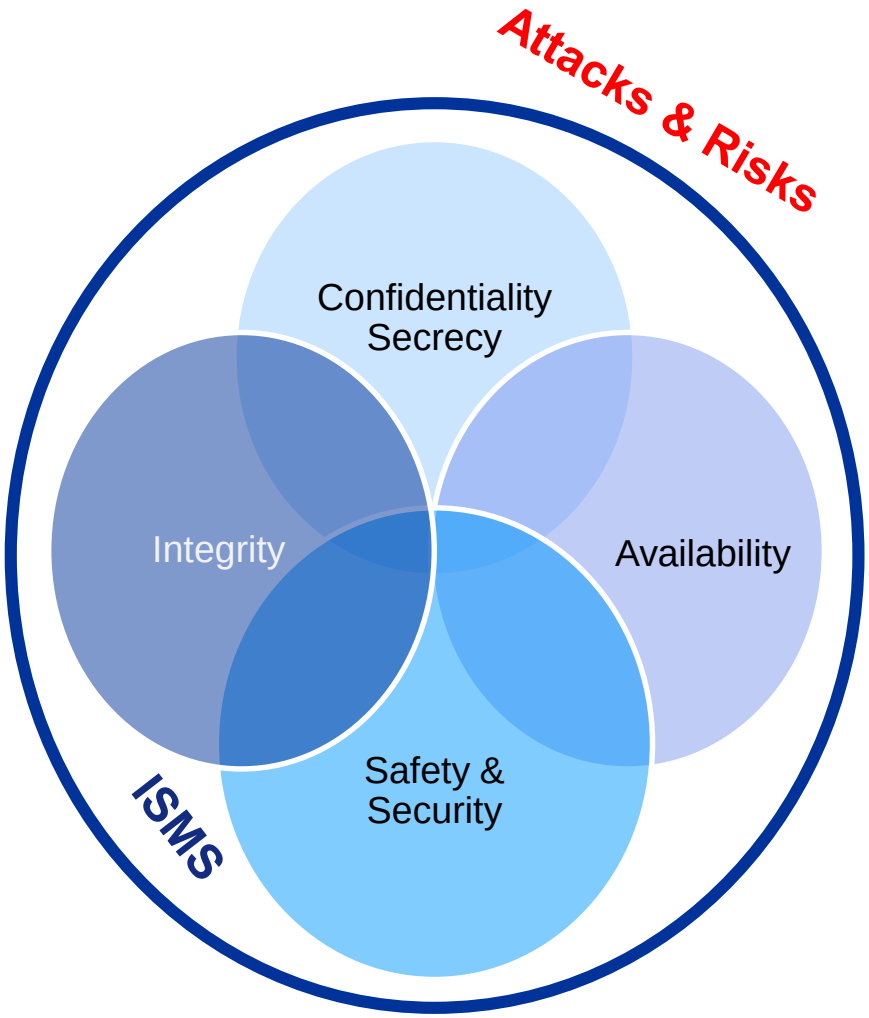
SYSTÉM MANAGEMENTU BEZPEČNOSTI INFORMACÍ V AUTOMOBILOVÉM PRŮMYSLU – TISAX

… další odpověď na výzvy a rizika moderní společnosti

TÜV NORD

ISMS JAKO ZÁKLAD PRO VYTVÁŘENÍ DŮVĚRY A ÚSPĚCHU V PODNIKÁNÍ

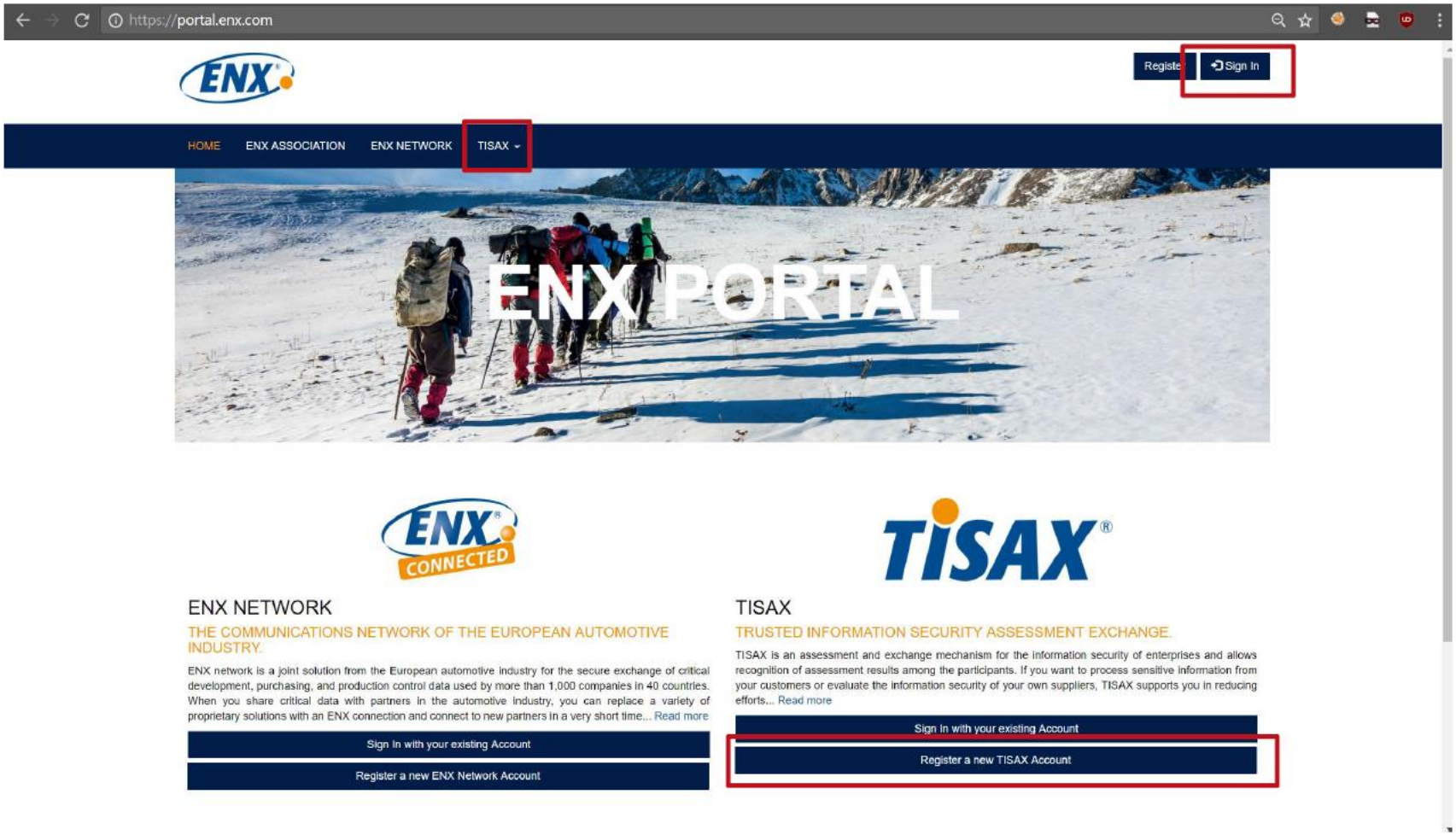
- digitalizace je základním faktorem úspěšného podnikání
- proto je důvěrnost, utajení, dostupnost, bezpečnost a integrita údajů a informací jsou pilířem kontinuity podnikání a důvěry
- různé "ideologie" a technologie mohou ohrozit tyto pilíře, např. kybernetické zločiny, terorismus atd.
- ISMS musí řešit tato rizika prostřednictvím nástrojů pro řízení rizik a kontinuity podnikání
- na ISMS se podílejí lidé i technologie, proto jde o rizikově orientovaný proces



CO JE TISAX?

- TISAX je zkratka pro Důvěryhodnou výměnu informací o hodnocení informační bezpečnosti (z angl. **T**rusted **I**nformation **S**ecurity **A**ssessment **Ex**change), byl vytvořen speciálně pro vytváření důvěryhodnosti v automobilovém průmyslu z důvodu narůstající digitalizace
- Německá VDA vydala základní požadavky pro hodnocení v podobě katalogu nástrojů Hodnocení informační bezpečnosti (**I**nformation **S**ecurity **A**ssessment - ISA)
- Katalog tvoří různé prvky které jsou odvozeny od rámce řízení a přílohy A normy ISO 27001, a dále od speciálních požadavků automobilového průmyslu:
  - ochrana prototypu
  - propojení s třetími stranami
  - ochrana údajů (právní shoda)
- Pro každý prvek musí být stanovena a hodnocena úroveň zralosti
- Podle citlivosti údajů a procesů jsou stanoveny a hodnoceny 3 stupně ochrany:
  - obvyklá ochrana
  - vysoká ochrana
  - velmi vysoká ochrana

TISAX/ENX PORTÁL



www.enx.com/

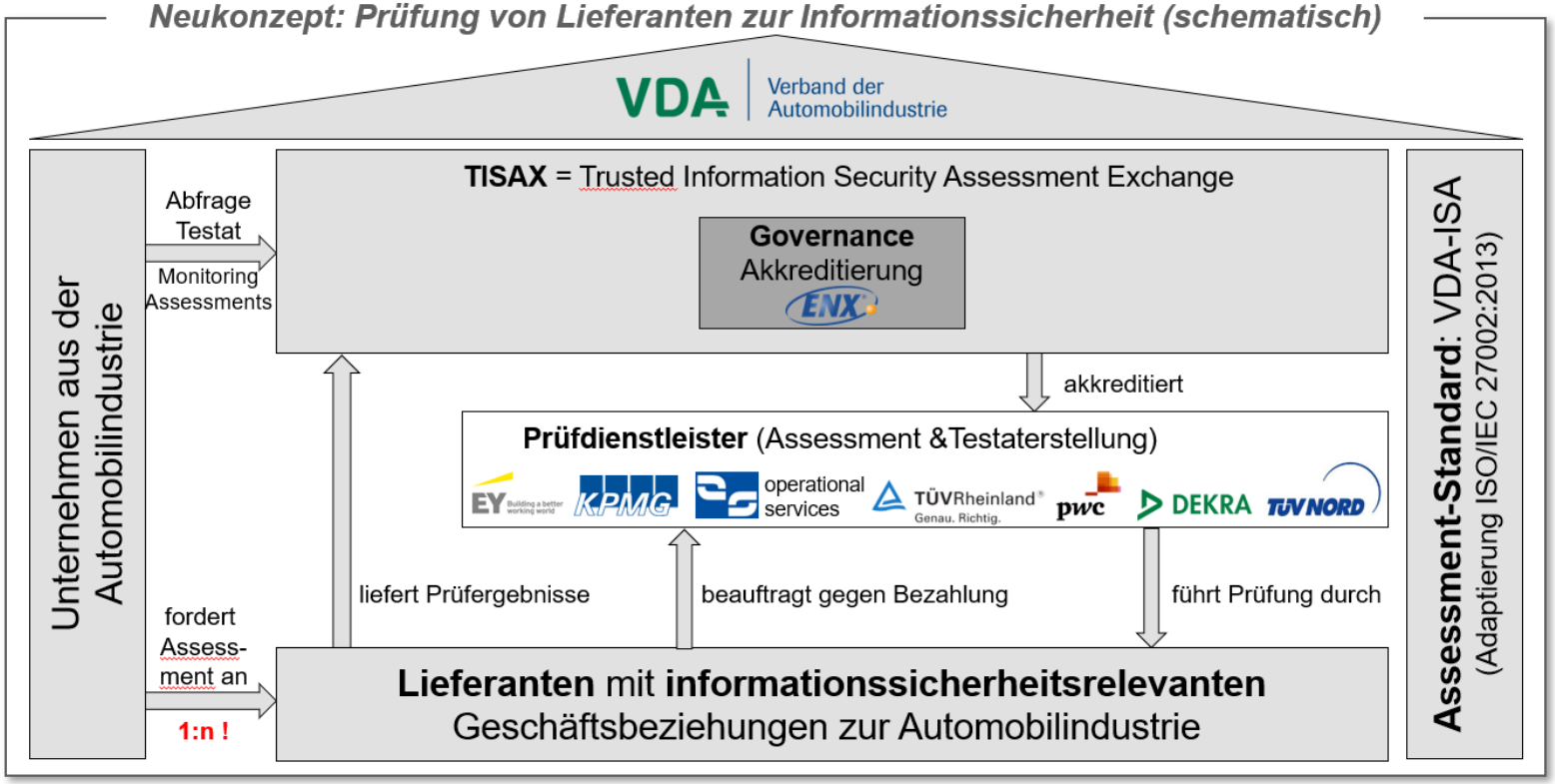
Source: ENX

POPIS PROCESU

Das TISAX-Modell ermöglicht eine IT-Sicherheitstestierung durch Prüfdienstleister nach VDA-Standard und trägt dazu bei, redundante Prüfungen zu vermeiden.

VDA

Neukonzept: Prüfung von Lieferanten zur Informationssicherheit (schematisch)



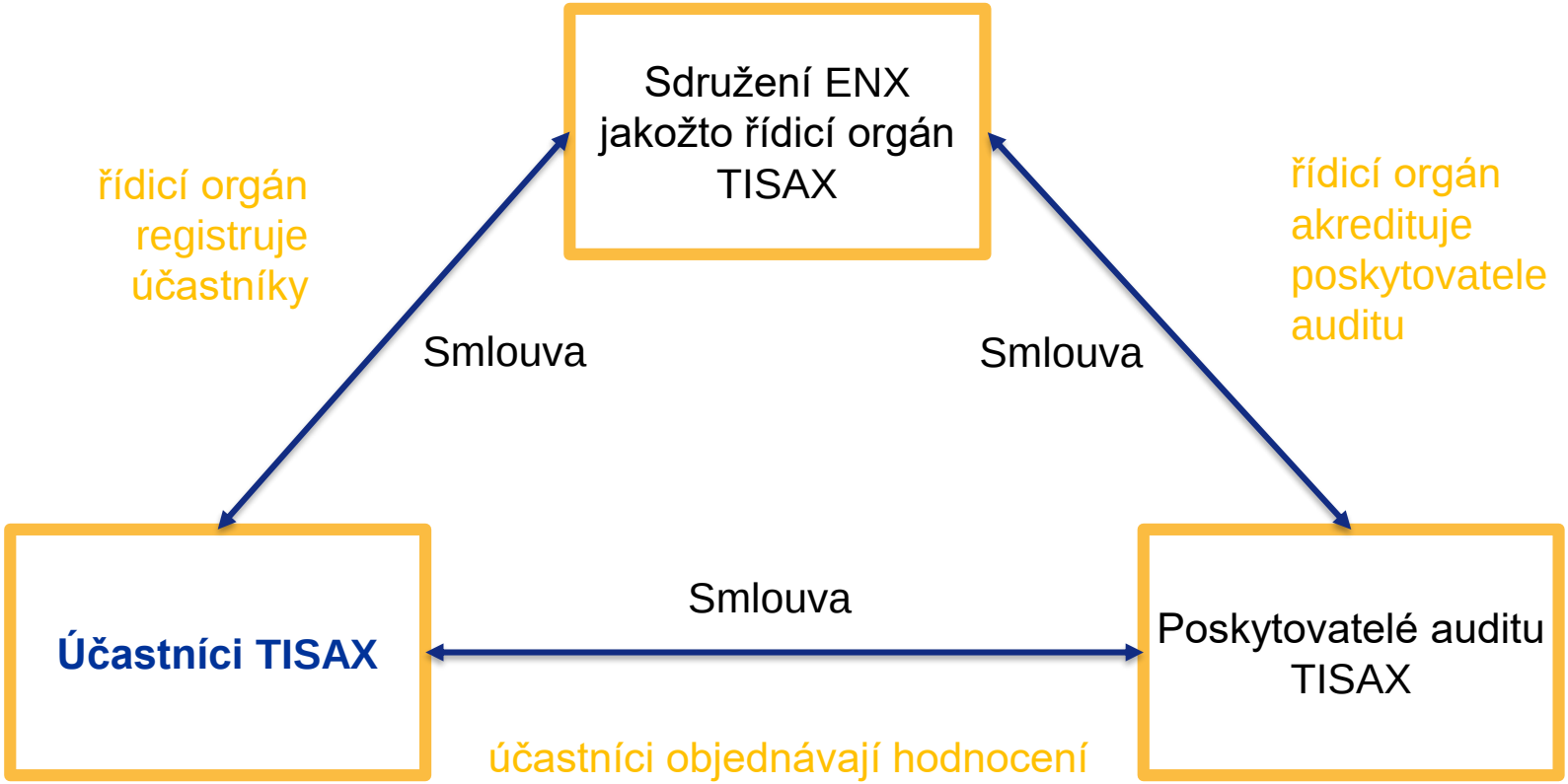
Source: VDA

TÜV NORD

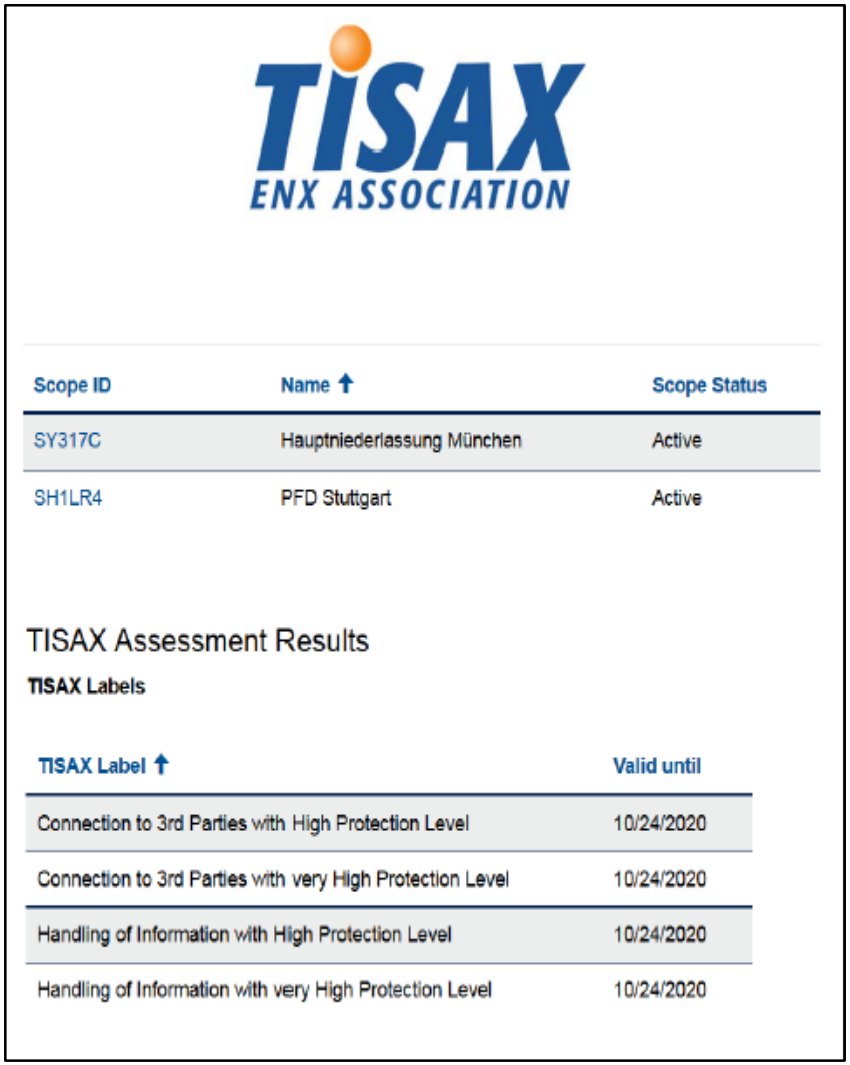
ÚLOHY V RÁMCI TISAX

- VDA je vlastníkem VDA-ISA a pověřila ENX řízením programu TISAX
- ENX je právním i organizačním operátorem hodnocení TISAX a související komunikační sítě
- TISAX program registruje více, než 1000 evropských výrobců a dodavatelů za 40 zemí
- akreditovaní poskytovatelé auditu TISAX (TISAX Accredited Audit Providers XAP) = certifikační orgány, jako např. TÜV NORD, kteří provádějí audity (hodnocení) 2.a 3. úrovně
- Zúčastněné strany musejí být registrovaní a mít uzavřenou smlouvu s ENX:
  → zákazníci - “pasivní” účastníci (např. zákazníci, kteří požadují po auditovaném hodnocení TISAX).
  → auditovaní - “aktivní” účastníci, mají přidělen:
  - ID účastníka
  - ID rozsahu (dle úrovně ochrany a očekávání zákazníka)
  - ID hodnocení (specifické pro každé hodnocení)
- Poradci mohou podporovat auditované, včetně účasti na auditu

TROJÚHELNÍK ŘÍZENÍ TISAX



CERTIFIKAČNÍ ZNAČKA TISAX



TISAX
ENX ASSOCIATION

Scope ID	Name ↑	Scope Status
SY317C	Hauptniederlassung München	Active
SH1LR4	PFD Stuttgart	Active

TISAX Assessment Results

TISAX Labels

TISAX Label ↑	Valid until
Connection to 3rd Parties with High Protection Level	10/24/2020
Connection to 3rd Parties with very High Protection Level	10/24/2020
Handling of Information with High Protection Level	10/24/2020
Handling of Information with very High Protection Level	10/24/2020

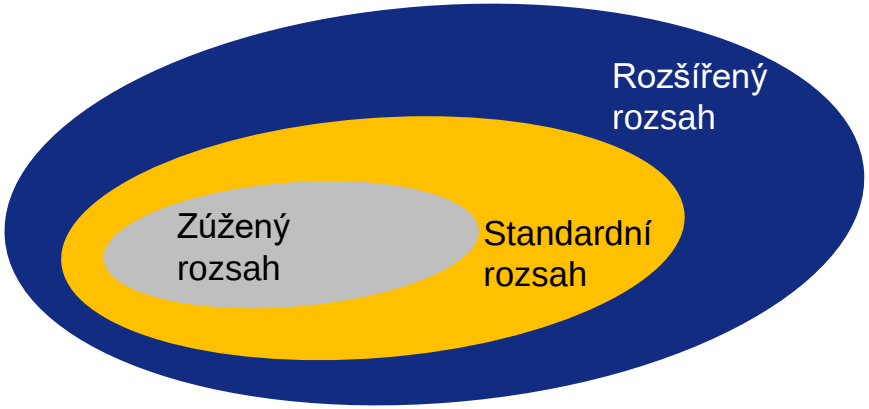
TÜV NORD

CÍLE TISAX

- Podle očekávání zákazníků auditovaných musí být kladen zvláštní důraz na:
  → definování rozsahu hodnocení ISMS
  (místa a skupiny, cíle i úrovně ochrany)
  → vzorkování a rozšíření / redukci rozsahu a míst
  → místa v zemích Aktivačního seznamu
- Certifikační značka koresponduje s cíli hodnocení, které jsou nastaveny na základě stupně zralosti a neshod
- Certifikační značka může být zveřejněna na internetové platformě TISAX na stránkách ENX, které jsou přístupné určeným účastníkům TISAX (zákazníkům, OEM)
- Hlavním cílem TISAX je minimalizace rizik a zvýšení transparentnosti dodavatelského řetězce prostřednictvím strukturovaného hodnocení, které poskytne spolehlivé údaje a informace, jakožto důkaz účinnosti ISMS.

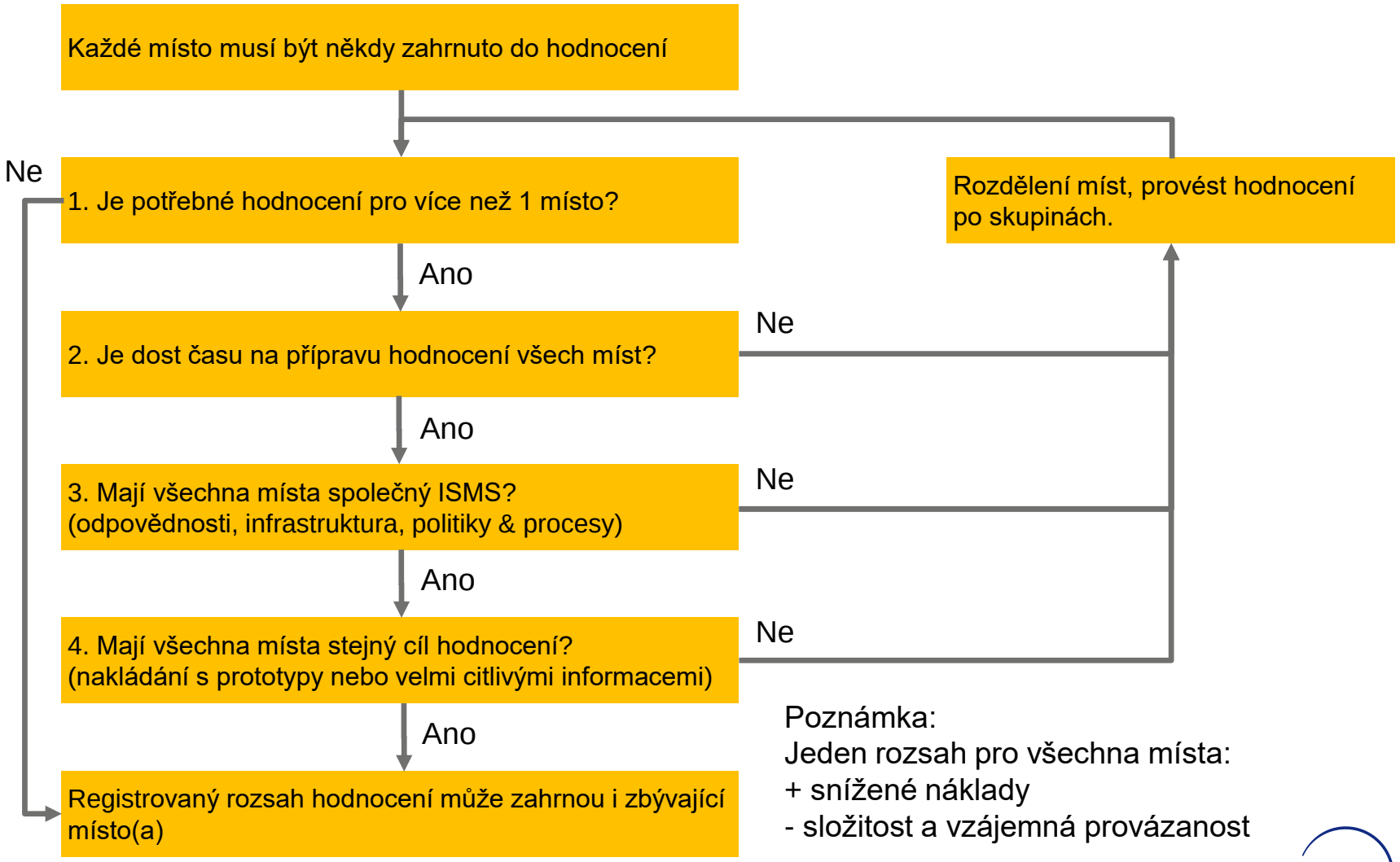
ROZSAH HODNOCENÍ TISAX

1. Standardní rozsah (doporučeno) …
   je základním východiskem pro hodnocení TISAX, a zahrnuje všechny procesy a relevantní zdroje v lokalitách (např. pracovní prostředky, IT systémy, zaměstnance, kanceláře, vývoj, výroba), které jsou zahrnuty do bezpečnostních požadavků partnerů (např. zákazníků).



2. Upravený rozsah …
   je buďto zúžený nebo rozšířený
   - zúžený rozsah je používán pro sdílenou infrastrukturu nebo pokud jsou výsledky hodnocení urgentně požadovány
     XAP omezuje množství a hloubku hodnocení – značka TISAX se nevydává
   - rozšířený rozsah může být použit, pokud je hodnocení TISAX použito pro interní procesy nebo mimo automobilový sektor.
     XAP používá více testů než pro standardní rozsah – značka TISAX může být vydána.

HODNOCENÍ TISAX – ROZSAHY MÍST



Poznámka:
Jeden rozsah pro všechna místa:
+ snížené náklady
- složitost a vzájemná provázanost

HODNOCENÍ TISAX – CÍLE

Cíle hodnocení jsou klíčovým vstupem procesů TISAX a jsou považovány za nástroj porovnání ISMS.
Zúčastněné strany na nich staví svou strategii hodnocení TISAX

Č.	Cíle hodnocení
1.	Informace s vysokým stupněm ochrany
2.	Informace s velmi vysokým stupněm ochrany
3.	Návaznost na 3. strany s vysokým stupněm ochrany
4.	Návaznost na 3. strany s velmi vysokým stupněm ochrany
5.	Nakládání s prototypy s vysokým stupněm ochrany
6.	Nakládání s prototypy s velmi vysokým stupněm ochrany
7.	Ochrana dat podle národního práva
8.	Ochrana dat se speciálními kategoriemi osobních údajů

ÚROVNĚ A CÍLE HODNOCENÍ TISAX

Úroveň hodnocení	Popis	Úroveň hodnocení
AL1	Sebehodnocení / Prohlášení auditovaného. Hodnocení prohlášení o sebehodnocení auditovaného.	Běžná ochrana
AL2	Verifikace sebehodnocení omezené na hodnocení důkazů a na pohovor s expertem (telefonický nebo osobní)	Vysoká ochrana
AL3	Úplné hodnocení včetně vyhodnocení důkazů, auditu na místě a pohovoru s expertem.	Velmi vysoká ochrana

TYPY HODNOCENÍ TISAX

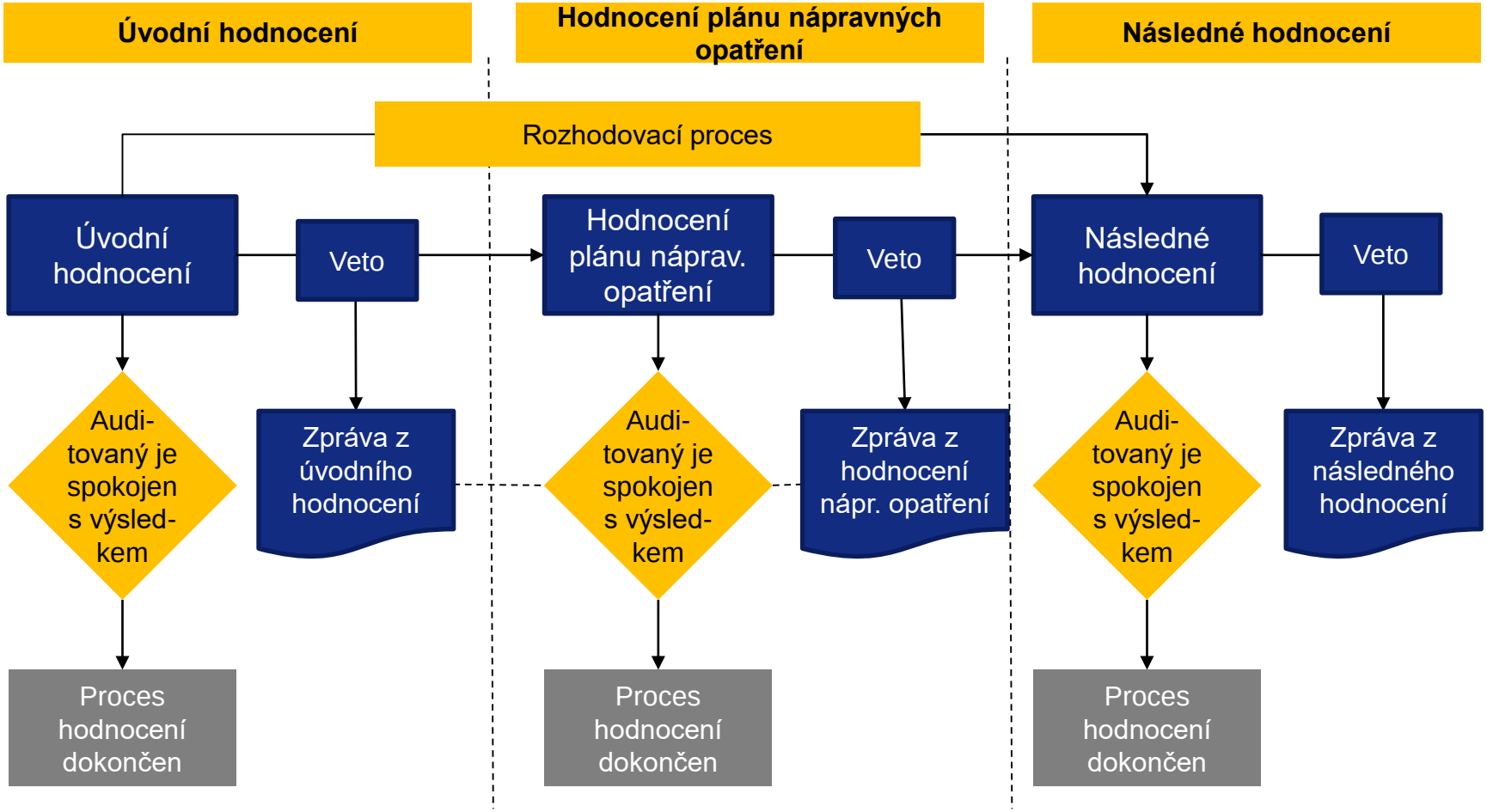
3 typy hodnocení TISAX:

1. Úvodní hodnocení
2. Hodnocení plánu nápravných opatření
3. Následné hodnocení

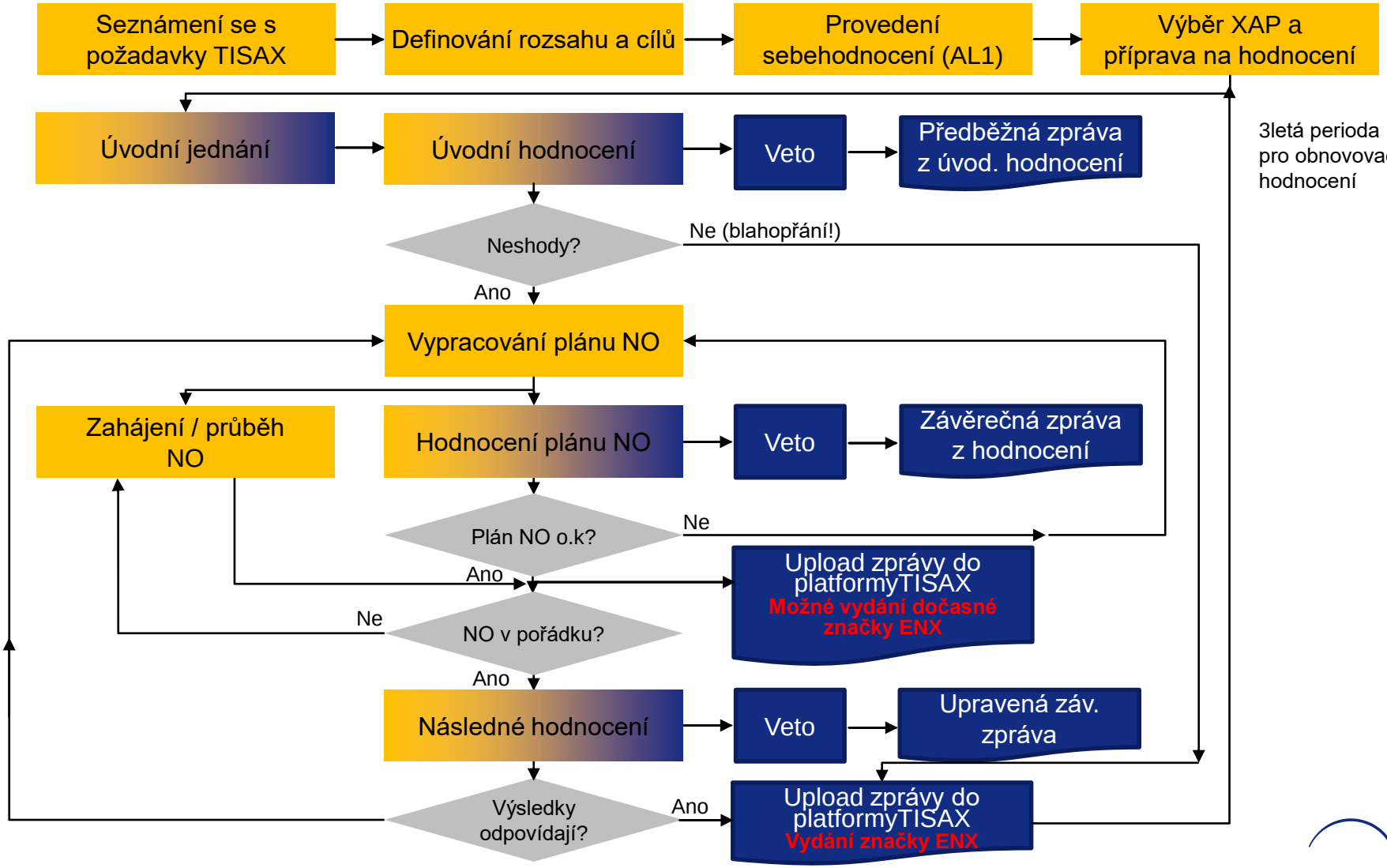
Hodnocení typu 2 a 3 se může provádět opakovaně
- buďto po uzavření všech neshod nebo
- pokud hodnocení bylo přerušeno nebo
- pokud byla dosažena lhůta 9 měsíců

Pozn.:
Překročení lhůty 9 měsíců vyžaduje nové úvodní hodnocení.

SMLUVNÍ FÁZE HODNOCENÍ TISAX : ÚVODNÍ, NÁPRAVNÁ A NÁSLEDNÁ OPATŘENÍ



HODNOCENÍ TISAX – PŘEHLED PROCESU



KATALOG TISAX – KAPITOLY ISMS (PŘÍLOHA A)

1. Všeobecné aspekty
5. Politiky informační bezpečnosti
6. Organizace bezpečnosti informací
7. Bezpečnost lidských zdrojů
8. Řízení aktiv
9. Řízení přístupu
10. Kryptografie
11. Fyzická bezpečnost a bezpečnost prostředí
12. Bezpečnost provozu
13. Bezpečnost komunikací
14. Akvizice, vývoj a údržba systému
15. Dodavatelské vztahy
16. Řízení incidentů bezpečnosti informací
17. Aspekty řízení kontinuity činností organizace z hlediska bezpeč. informací
18. Soulad s požadavky

TISAX – DOPLŇKOVÉ KATALOGY

Doplňkový katalog	Popis	Požadavky a poznámky
Návaznost na 3. strany	Požadováno, pokud dodavatelé nebo poskytovatelé služeb (3. strany) si pronajali prostory v OEM zařízeních a pokud má tento majetek napojení na externí firemní síť	Požadováno hodnocení na místě, pouze AL2 nebo AL3
Ochrana prototypu	Požadavky spojené s prototypy nebo s jejich součástmi	Požadováno hodnocení na místě, pouze AL2 nebo AL3
Ochrana údajů	Dle §11 Bundesdatenschutz-gesetz (smluvní procesování údajů)	příp. AL3

TISAX – DOPLŇKOVÉ KATALOGY – KAPITOLY

Návaznost na 3. strany

23.7 Bezpečnost lidských zdrojů

23.9 Řízení přístupu

23.11 Fyzická bezpečnost a bezpečnost prostředí

23.13 Bezpečnost komunikací

Ochrana prototypu

25.1 Fyzická bezpečnost a bezpečnost prostředí

25.2 Organizační požadavky

25.3 Nakládání s protypy

Ochrana údajů

(Doplňující otázky k ochraně údajů při jejich smluvním zpracování podle § 11 BDSG)

TISAX – VÝSLEDKY A ÚROVNĚ ZRALOSTI

- Úrovně zralosti se používají pro známkování kvality ISMS.
- Sebehodnocení VDA-ISA definuje 6 úrovní zralosti, k nimž se vztahují všechny otázky a katalogová kritéria.
- Kromě vlastní definice jsou požadavky popsány formou návrhu nejlepší (správné) praxe, ty jsou jedinečné pro každou otázku.
- Pro konsolidovaný pohled na úrovně zralosti jsou k dispozici následující zjednodušená shrnutí:

TISAX – ÚROVNĚ ZRALOSTI (SOUHRN)

Úroveň		Popis
0	Neúplná	Zavedení požadavků je neúplné, procesy zatím nejsou k dispozici nebo nedosahuje požadovaných výsledků.
1	Funkční	Požadavky nezbytné k relevantní ochraně informací jsou prováděny, procesy jsou zavedeny a vykazují známky funkčnosti. Nejsou však plně dokumentovány, takže není nelze zaručit jejich funkčnost za všech okolností.
2	Řízená	Procesy dosahování cílů jsou zavedeny a dokumentovány, důkazy jsou k dispozici (např. dokumentace).
3	Zavedená	Procesy dosahování cílů jsou zavedeny a propojeny tak, aby ukázaly existující závislosti. Dokumentace je aktuální a udržována.
4	Předvídatelná	Požadavky z úrovně 3 plus měření výsledků (např. jako KPI) tvoří předvídatelnost procesů.
5	Optimalizovaná	Požadavky z úrovně 4 plus další zdroje (např. lidské, finanční) jsou k dispozici v optimální podobě. Procesy jsou směrovány k neustálému zlepšování.

TISAX – PAVUČINA ZRALOSTI

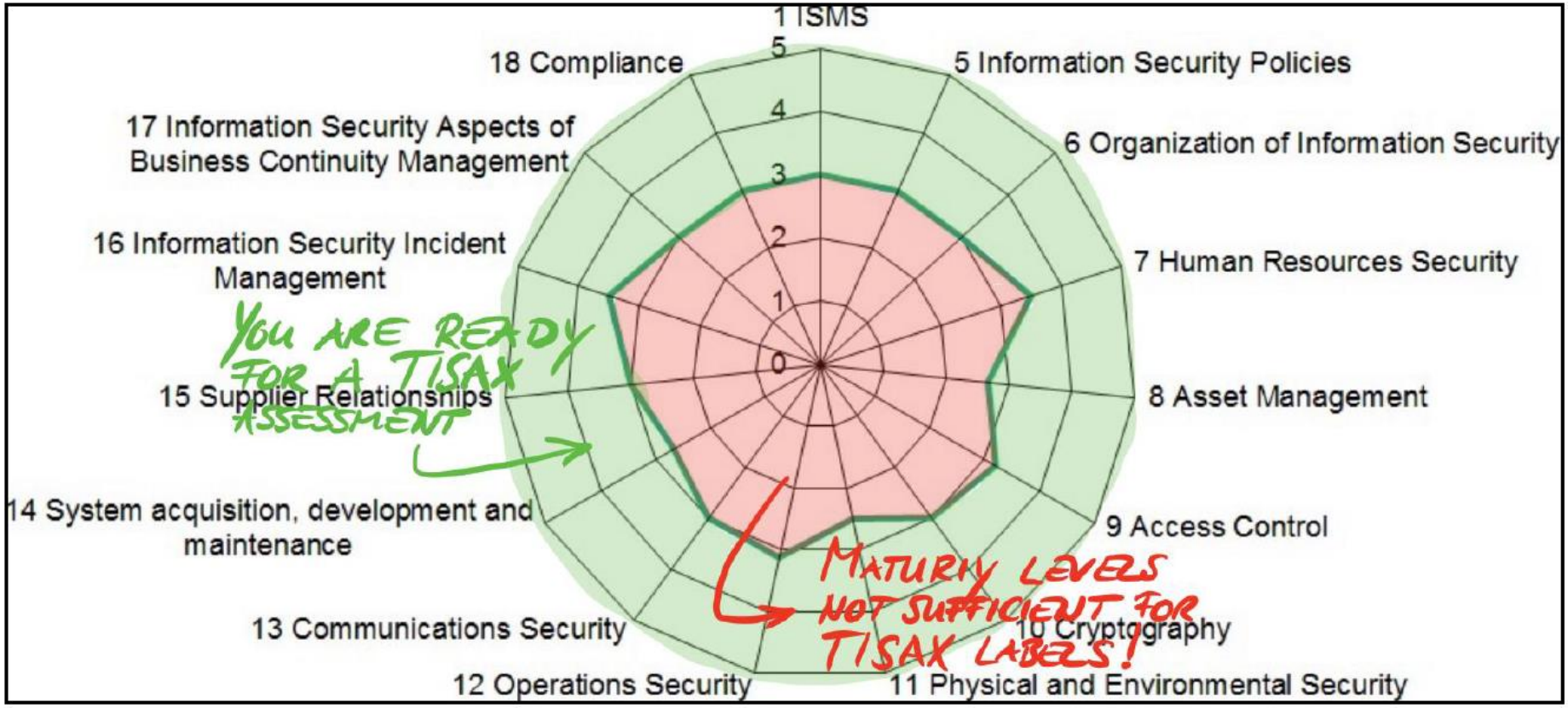


Figure 18: VDA-ISA spider web diagram: Target maturity level

TISAX – KLASIFIKACE ZJIŠTĚNÍ

Klasifikace	Definice
Velká neshoda	Neshoda s jedním nebo více požadavky, která zpochybňuje celkovou efektivitu ISMS nebo indikuje závažné riziko v oblasti bezpečnosti informací.
Malá neshoda	Izolované nebo jednotlivé odchylky. Neshody nebo nedostatky v implementaci požadavků nebo vlastních standardů, které nezpochybňují celkovou efektivitu ISMS ani neindikují závažné riziko v oblasti bezpečnosti informací.
Pozorování	Odchylná zjištění, která nemohou být klasifikována jako neshody s požadavky nebo s vlastními standardy, avšak musí být dále pod zvýšeným dohledem, aby nezvyšovala riziko pro bezpečnost informací.
Zlepšení	Odchylná zjištění, která nemohou být klasifikována jako neshody či pozorování a nemohou vést k ohrožení bezpečnosti informací, nicméně poskytují potenciál pro zlepšování.

TISAX – ŘÍZENÍ NESHOD

Klasifikace	Požadovaná opatření a důsledky
Velká neshoda	Požadavek na okamžitá opatření / nápravu a plán nápravných opatření. Pokud je provedena náprava a je zpracován plán nápravných opatření, je možný downgrade neshody na malou. Aby mohla být neshoda zcela uzavřena, je třeba realizovat relevantní plán opatření a poté provést následné hodnocení. Značka TISAX nemůže být vydána, pokud velká neshoda přetrvává.
Malá neshoda	Aby mohla být malá neshoda zcela uzavřena, je třeba realizovat relevantní plán opatření a poté provést následné hodnocení. Provizorní značka TISAX může být vydána (a jako taková akceptována).
Pozorování	Žádná
Zlepšení	Doporučená

HODNOCENÍ TISAX – CELKOVÉ VÝSLEDKY

1. Odchylky aktuální úrovně od cílené úrovně zralosti do 10% lze tolerovat, dokud není známo bezpečnostní riziko.

2. Odchylky aktuální úrovně od cílené úrovně zralosti nad 30% je nutno klasifikovat jako velkou neshodu, bez ohledu na přítomnost bezpečnostního rizika.

3. Několik malých neshod, které indikují systémový problém ISMS, musí být klasifikovány jako velká neshoda.

4. Velké neshody, na které byla patřičná odezva zahrnující eliminaci hrozby mohou být re-klasifikovány na malé neshody.

VÝHODY HODNOCENÍ TISAX – SHRNUTÍ

- Poskytuje přehled o kvalitě a zralosti ISMS a orientace ve nejlepší praxi.
- Stanovení rozsahu, hodnocení a proces výměny informací jsou adekvátně nastaveny k uspokojení zákazníků (pasivních účastníků) :
  - transparentní hodnocení
  - standardizované, porovnatelné a smysluplné výsledky
  - zaměření na snižování rizik a důvěryhodnost
  - podporují stávající a nové vztahy mezi obchodními partnery
- Je akceptován širokým okruhem účastníků TISAX.
- Plná kontrola nad výsledky hodnocení ze strany auditovaných.
- TISAX může být cesta k úplné certifikace podle ISO 27001 a je tudíž významným příspěvkem k řízení a snižování rizik.

TISAX – Řízení bezpečnosti informací

Děkujeme za pozornost i za dotazy.

Viktor Šaroch
saroch@tuev-nord.cz

Frank Lürkens
fluerkens@tuev-nord.de

TÜV NORD Czech, s.r.o., Českomoravská 2420/15, 190 00 Praha 9 – Libeň
www.tuev-nord.cz