TISAX® – standard v automobilovém průmyslu

Ing. Martin Drastich MBA, Ph.D.

TISAX®

TÜVNORD

1. ISO/IEC 27001:2013 resp. ČSN EN ISO/IEC 27001:2014 nově
   ISO/IEC 27001:2021 resp. ČSN EN ISO/IEC 27001:2022

2. Zákon 181/2014 sb. O kybernetické bezpečnosti
   + vyhláška 82/2018 sb. O kybernetické bezpečnosti
   + vyhláška č. 317/2014 sb., O významných IS
   NIS2 (Network Information Security) – 16. říjen 2024

3. TISAX - Trusted Information Security Assessment Exchange, zkráceně TISAX, je druh certifikace sloužící k prokázání bezpečnosti informací mezi spolupracujícími společnostmi v automobilovém průmyslu.
V minulosti verze VDA ISA 5.1 (41 oblastí) od 1.4.2024 nově VDA ISA 6.0 (46 oblastí)

Stupně - AL1 (standard), AL2 (High), AL3 (Very High Protection Level)
Vybrané pasáže z ISMS – 27001 + 1-7. Information Security
+ 8. Prototype Protection
+ 9. Data Protection

TISAX®

TÜVNORD

8.800
TISAX Participants

18
TISAX Audit Providers

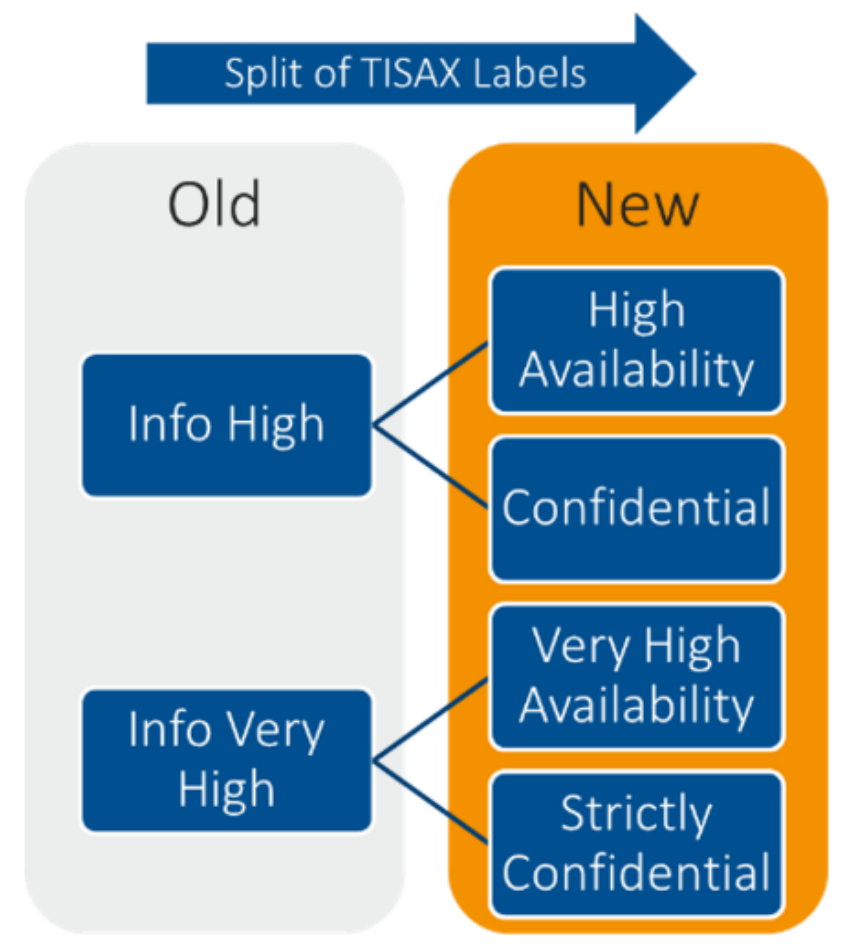
>50.000
Improvements of information security since 2018

Among them >5000 critical risks that could be identified and addressed

18.800
Registered Locations

11.500
Assessed Locations with valid labels

TISAX®



Nové Labely – „availability“ a „confidential“

V poslední době získala pozornost významná hrozba – útoky ransomware

I když je to také hrozba pro důvěrnost, může mít způsobená škoda ovlivněná dostupností ještě větší dopad.

Největší škody ve výrobě jsou způsobeny výpadky dodávek produktů a služeb v dodavatelském řetězci

TISAX®

TÜVNORD

Requested asessment objectives/Labels		Selection
Confidential	Confidential Information	n
Strictly Confidential	Strictly Confidential Information	n
Avail High	High Availability	n
Avail Very High	Very High Availability	n
Data	Data Protection	n
Special Data	Data Protection with Special Categories of Personal Data	n
Proto Parts	Protection of Prototype Parts and Components	n
Proto Vehicles	Protection of Prototype Vehicles	n
Test Vehicles	Handling of Test Vehicles	n
Proto Events	Protection of Prototypes durings Events and Film or Photo Shoots	n

TISAX®

TÜVNORD

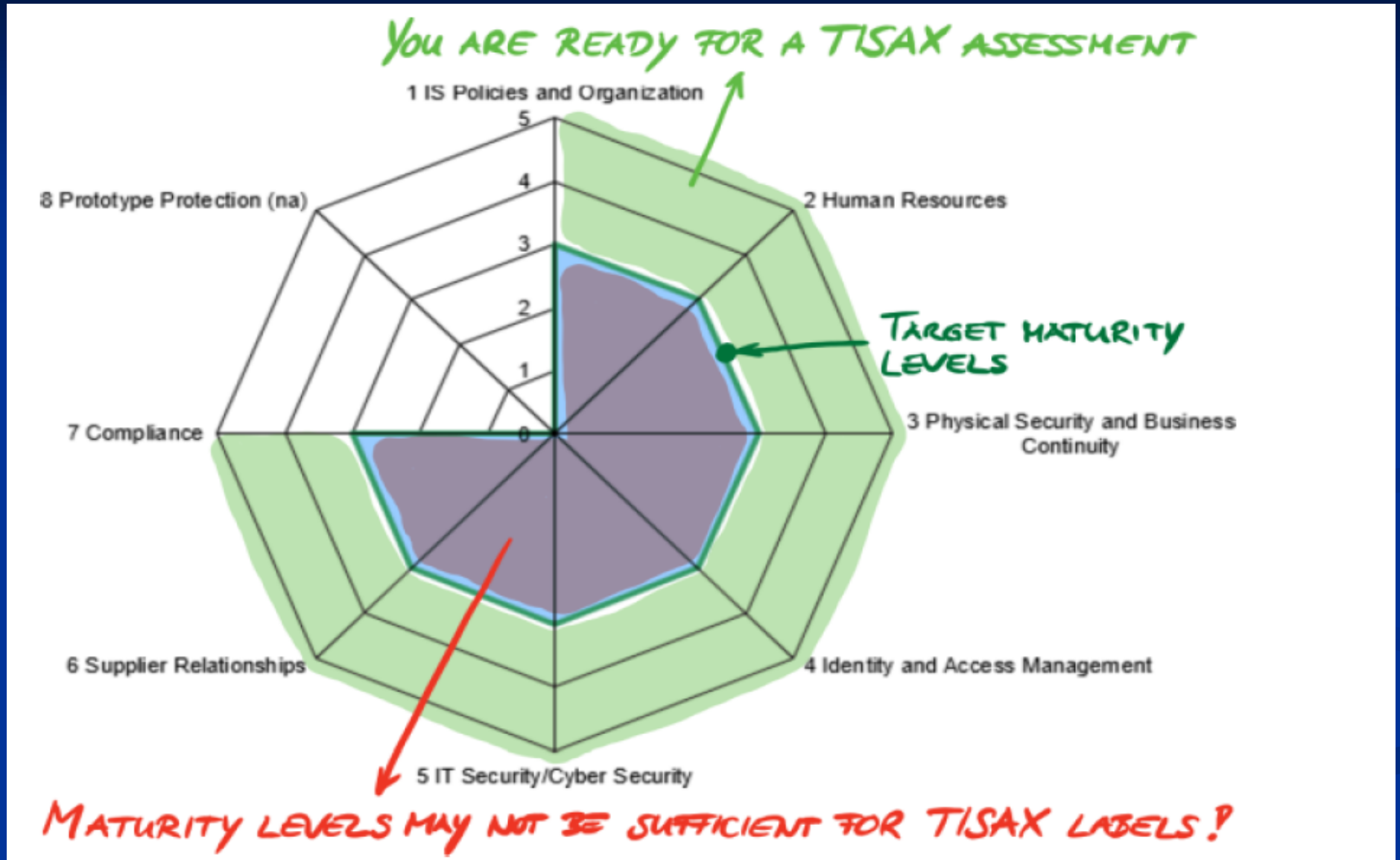
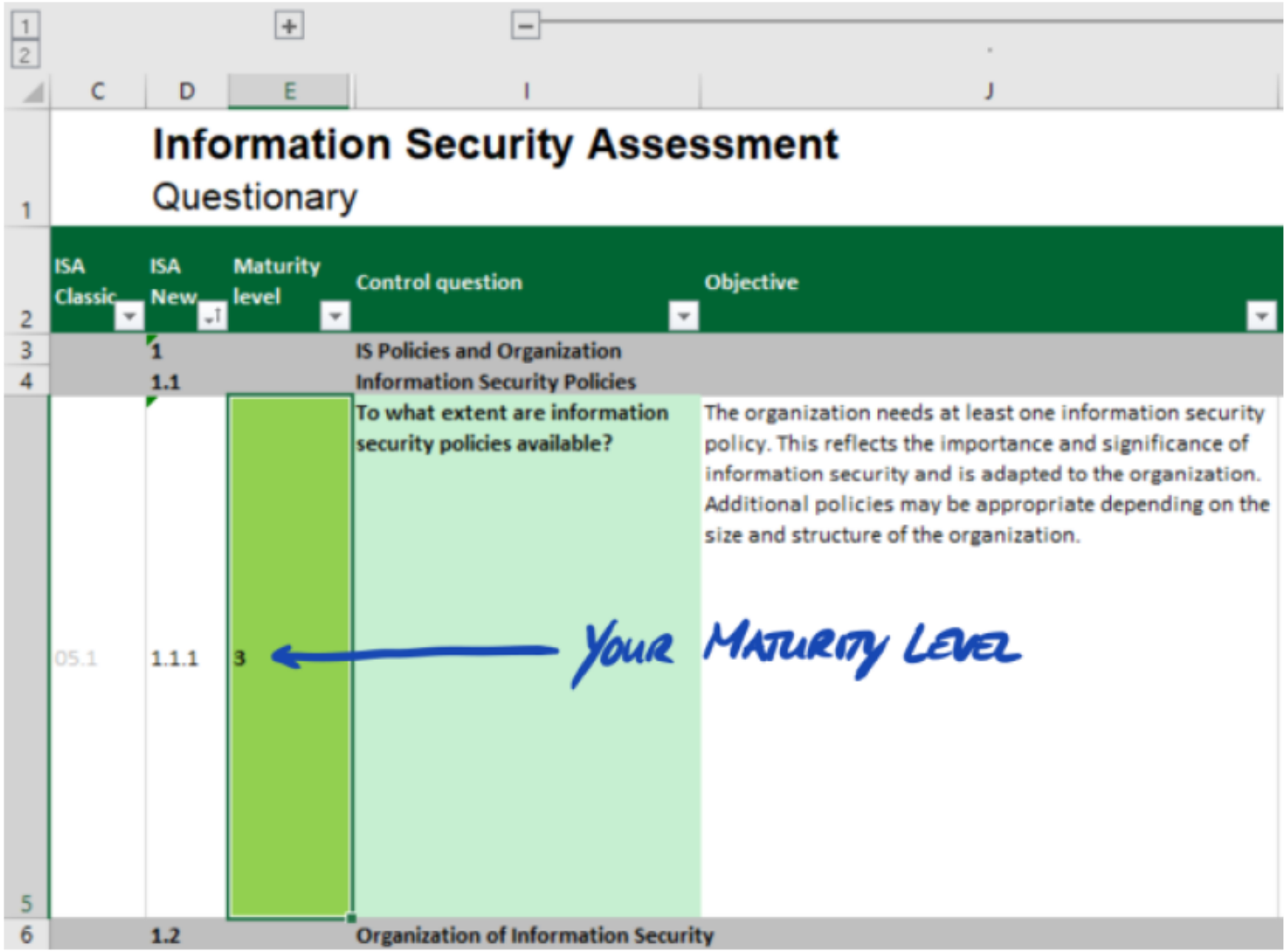


Figure 30. Screenshot: Target maturity level fulfilment in the ISA spider web diagram (Excel sheet "Results (ISA5)")



Information Security Assessment

Questionary

ISA Classic	ISA New	Maturity level	Control question	Objective
	1		IS Policies and Organization	
	1.1		Information Security Policies	
05.1	1.1.1	3	To what extent are information security policies available?	The organization needs at least one information security policy. This reflects the importance and significance of information security and is adapted to the organization. Additional policies may be appropriate depending on the size and structure of the organization.
	1.2		Organization of Information Security	

Figure 15. Screenshot: Example of maturity level selection in the ISA document (Excel sheet "Information Security")

TISAX®

Maturity level

TÜVNORD

Level	Name	Description
0	Incomplete	There is no process, or the process does not work. Neexistuje žádný proces nebo proces nefunguje
1	Performed	There is a process and the result shows it works, but the process is not documented and nobody knows for sure why the process works. Existuje proces a výsledek ukazuje, že funguje, ale tento proces není zdokumentován a nikdo neví, proč tento proces funguje.
2	Managed	There are processes that work and are documented, but there are different processes for the same objective. Existují procesy, které fungují a jsou dokumentovány, ale pro stejný cíl existují různé procesy.
3	Established Implemented	There is a process that works and has documentation that is up-to-date and maintained. Existuje proces, který funguje a má dokumentaci, která je aktuální a udržovaná.
4	Predictable	Same as for level 3, plus the process is measured. 3 plus měří se procesy.
5	Optimizing	Same as for level 4, plus dedicated staff is responsible for continual improvements. 4 plus odpovědný personál je zodpovědný za neustálé zlepšování.

TISAX®

TÜVNORD

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

GREEN = ✓

No.	Subject	Target maturity	Result
1.1.1	Do jaké míry jsou k dispozici zásady zabezpečení informací?	3	
1.2.1	Do jaké míry je v organizaci spravována informační bezpečnost?	3	
1.2.2	Do jaké míry jsou organizovány odpovědnosti za bezpečnost informací?	3	
1.2.3	Do jaké míry jsou v projektech brány v úvahu požadavky na bezpečnost informací?	3	
1.2.4	Do jaké míry jsou definovány odpovědnosti mezi externími poskytovateli služeb IT a vlastní organizací?	3	
1.3.1	Do jaké míry jsou informační aktiva identifikována a zaznamenána?	3	
1.3.2	Do jaké míry jsou informační aktiva klasifikována a spravována z hlediska jejich potřeb ochrany?	3	
1.3.3	Do jaké míry je zajištěno, že ke zpracování informačních aktiv organizace jsou použity pouze hodnocené a schválené externí služby IT?	3	
1.4.1	Do jaké míry jsou rizika zabezpečení informací řízena?	3	
1.5.1	Do jaké míry je zajištěn soulad s informační bezpečností v postupech a procesech?	3	
1.5.2	Do jaké míry je ISMS přezkoumáván nezávislým subjektem?	3	

TISAX®

TÜVNORD

Reference to ISO 27001: 4
Reference to ISO 27001: 6.1.2, 6.1.3
Reference to ISO 27001: A.5.1.1, A.5.1.2
Reference to ISO 27001: A.6.1.1
Reference to ISO 27001: A.6.1.5
Reference to ISO 27001: A.6.2
Reference to ISO 27001: A.6.2, A.8.3
Reference to ISO 27001: A.7.1.1
Reference to ISO 27001: A.7.1.2, A.7.3.1
Reference to ISO 27001: A.7.2.1, A.7.2.2
Reference to ISO 27001: A.8.1.1, A.8.1.2
Reference to ISO 27001: A.8.1.3, A.8.1.4
Reference to ISO 27001: A.8.2.1, A.8.2.2, A.8.2.3
Reference to ISO 27001: A.9.1., A.9.4.2
Reference to ISO 27001: A.9.2.1, A.9.2.2, A.9.2.4, A.
Reference to ISO 27001: A.9.2.3, A.9.2.5, A.9.4.1
Reference to ISO 27001: A.9.2.6
Reference to ISO 27001: A.10.1.
Reference to ISO 27001: A.11.1
Reference to ISO 27001: A.12.1.2
Reference to ISO 27001: A.12.1.4
Reference to ISO 27001: A.12.2
Reference to ISO 27001: A.12.3, A.17.1, A.17.2
Reference to ISO 27001: A.12.4.1, A.12.4.2, A.12.4.3
Reference to ISO 27001: A.12.6
Reference to ISO 27001: A.12.7, A.18.2.3
Reference to ISO 27001: A.13.1.1, A.13.1.3
Reference to ISO 27001: A.13.1.2
Reference to ISO 27001: A.13.2.1, A.13.2.3
Reference to ISO 27001: A.13.2.2, A.13.2.4
Reference to ISO 27001: A.14.1
Reference to ISO 27001: A.15.1, A.15.2.1
Reference to ISO 27001: A.16.1.
Reference to ISO 27001: A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.5
Reference to ISO 27001: A.18.1.4
Reference to ISO 27001: A.18.2.1
Reference to ISO 27001: A.18.2.2, A.18.2.3
Reference to ISO 27017: CLD 14.1.1
Reference to ISO 27017: CLD.6.3.1
Reference to ISO 27017: CLD.8.1.5
Reference to ISO 27017: CLD.9.5.1, CLD.9.5.2

Co je to informační bezpečnost?

Zbožím naší doby se staly informace

Informace jsou aktiva která, jako jiná důležitá podnikatelská aktiva, mají pro organizaci hodnotu, a tudíž musí být odpovídajícím způsobem chráněny.

Co je to informační bezpečnost?

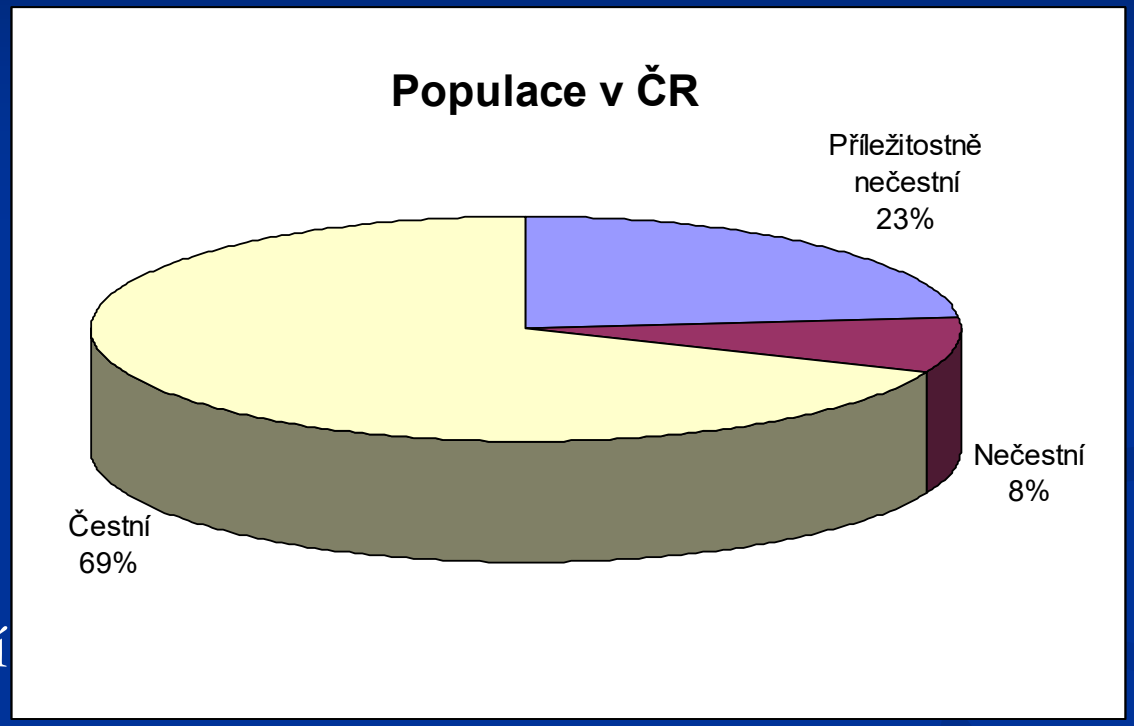
- ✓ El. informace uložené v počítačových systémech.
- ✓ Tištěné nebo psané informace v papírové formě.

Druhy informací

- ✓ Mluvené slovo.
- ✓ Informace na videu nebo na zvukovém záznamu.

Co je to informační bezpečnost?

Graf MV ČR



- ✓ 67% čestní,
- ✓ 8% nečestní,
- ✓ 25% příležitostně nečestní

je navenek zcela loajálních a jeví se jako čestní, ale pod tlakem okolností mohou sáhnout k nečestným praktikám. Okolnosti, které k tomu donutí, jsou různé, od lásky k nenávisti, od nedostatku peněz k jejich nadbytku a z toho plynoucí morální degradaci.

Co je to informační bezpečnost?

Confidentiality – důvěrnost.

Integrity – integrita.

Availability – dostupnost.

Zachování důvěrnosti, integrity a dostupnosti.

TISAX®

CISO, Manažer/zmocněnec nebo pověřenec bezpečnosti

Management

Manažer

Řízení
Organizování
Prezentování

Správa ICT

Administrátor

Administrace
Instalování
Programování

TÜVNORD

TISAX®

1.1 Information Security Policies

1.1.1 **To what extent are information security policies available?**

Do jaké míry jsou dostupné zásady bezpečnosti informací?

Organizace potřebuje alespoň jednu politiku zabezpečení informací. To odráží důležitost a význam informační bezpečnosti a je přizpůsobeno organizaci. V závislosti na velikosti a struktuře organizace mohou být vhodné další zásady.

ISO 27002

a) řízení přístupu (viz kapitola 9);
b) klasifikaci informací (a zacházení s informacemi) (viz 8.2);
c) fyzickou bezpečnost a bezpečnost prostředí (viz kapitola 11);
d) témata orientovaná na koncového uživatele, jako jsou:
   1) přijatelné použití aktiv (viz 8.1.3);
   2) čistý stůl a čistý displej (viz 11.2.9);
   3) přenos informací (viz 13.2.1);
   4) mobilní zařízení a práce na dálku (viz 6.2);
   5) omezení týkající se instalací a použití softwaru (viz 12.6.2);
e) zálohování (viz 12.3);
f) přenos informací (viz 13.2);
g) ochrana před malwarem (viz 12.2);
h) správa a řízení technických zranitelností (viz 12.6.1);
i) kryptografická opatření (viz kapitola 10);
j) bezpečnost komunikací (viz kapitola 13);
k) soukromí a ochrana osobních údajů (viz 18.1.4);
l) dodavatelské vztahy (viz kapitola 15).

1.2 Organization of Information Security

1.2.1 **To what extent is information security managed within the organization?**

Do jaké míry je v organizaci řízena infformační bezpečnost?

Pouze pokud je informační bezpečnost součástí strategických cílů organizace, může být informační bezpečnost v organizaci implementována udržitelným způsobem. Systém řízení informační bezpečnosti (ISMS) je kontrolní mechanismus používaný managementem organizace k zajištění toho, že informační bezpečnost je výsledkem udržitelného řízení spíše než pouhé náhody a individuálního úsilí.

1.2 Organization of Information Security

1.2.2 **To what extent are information security responsibilities organized?**
Do jaké míry jsou organizovány odpovědnosti za bezpečnost informací?
Úspěšný ISMS vyžaduje jasné odpovědnosti v rámci organizace.

1.2.3 **To what extent are information security requirements considered in projects?**
Do jaké míry jsou v projektech zohledňovány požadavky na bezpečnost informací? For Pro realizaci projektu je důležité zvážit požadavky na bezpečnost informací. To platí pro projekty v rámci organizace bez ohledu na jejich typ. Vhodným nastavením procesu informační bezpečnosti v postupech projektového řízení organizace se zabrání jakémukoli přehlížení požadavků.

1.2.4 **To what extent are the responsibilities between external IT service providers and the own organization defined?**
Do jaké míry jsou definovány odpovědnosti mezi externími poskytovateli IT služeb a vlastní organizací?
Je důležité, aby existovalo společné chápání rozdělení odpovědností a aby byla zajištěna implementace všech bezpečnostních požadavků. Proto při využívání externích poskytovatelů IT služeb a IT služeb musí být definovány a ověřitelně zdokumentovány odpovědnosti za implementaci opatření informační bezpečnosti.

1.3 Asset Management

1.3.1 **To what extent are information assets identified and recorded?**

Do jaké míry jsou identifikována a evidována informační aktiva?

„Pro každou organizaci je důležité znát informace, které tvoří její základní aktiva (např. obchodní tajemství, kritické obchodní procesy, know-how, patenty).
Označují se jako informační aktiva. Inventarizace zajišťuje, že organizace získá přehled o svých informačních aktivech.
Kromě toho je důležité znát podpůrná aktiva (např. IT systémy, služby/služby IT, zaměstnanci) zpracovávající tato informační aktiva."

1.3.2 **To what extent are information assets classified and managed in terms of their protection needs?**

Do jaké míry jsou informační aktiva klasifikována a spravována z hlediska potřeb jejich ochrany?

Cílem klasifikace informačních aktiv je důsledné stanovení potřeb jejich ochrany. Pro tento účel je hodnota, kterou informace pro organizaci mají, určena na základě cílů ochrany bezpečnosti informací (důvěrnost, integrita a dostupnost) a klasifikována podle klasifikačního schématu. To umožňuje organizaci zavést adekvátní ochranná opatření.

1.3 Asset Management

1.3.3 **To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?**

Do jaké míry je zajištěno, že se pro zpracování informačních aktiv organizace používají pouze vyhodnocené a schválené externí IT služby?

Zejména v případě externích IT služeb, které lze využívat za relativně nízké náklady nebo zdarma, existuje zvýšené riziko, že pořízení a uvedení do provozu budou provedeny bez náležitého zohlednění požadavků na bezpečnost informací, a tudíž nebude zajištěna bezpečnost.

1.3.4 **To what extent is it ensured that only evaluated and approved software is used for processing the organization's information assets? New 6.0**

Do jaké míry je zajištěno, že se pro zpracování informačních aktiv organizace používá pouze vyhodnocený a schválený software?

Zpracování informací se většinou provádí pomocí specifického softwaru. Bezpečnostní problémy v softwaru se snadno stanou rizikem pro zpracovávané informace. V souladu s tím musí být software náležitě spravován.

1.4 IS Risk Management

1.4.1 **To what extent are information security risks managed?**

Do jaké míry jsou řízena rizika informační bezpečnosti?

Řízení rizik informační bezpečnosti se zaměřuje na včasnou detekci, hodnocení a řešení rizik za účelem dosažení cílů ochrany informační bezpečnosti. Umožňuje tak organizaci zavést adekvátní opatření na ochranu svých informačních aktiv s ohledem na související vyhlídky a rizika. Doporučuje se udržovat řízení rizik informační bezpečnosti organizace co nejjednodušší, aby bylo možné její efektivní a efektivní provoz.

ISO 27005

B.1 Příklady identifikace aktiv

B.1.1 Obecně

Aby provedla ocenění aktiv, potřebuje organizace nejprve identifikovat svá aktiva (na příslušné úrovni podrobnosti). Mohou být rozlišovány dva druhy aktiv:

- primární aktiva:
  - podnikatelské procesy a činnosti;
  - informace;
- podpůrná aktiva (na která se spoléhají primární prvky v oblasti působnosti) všech typů:
  - hardware;
  - software;
  - síť;
  - zaměstnanci;
  - lokalita;
  - struktura organizace.

1.5 Assessments

1.5.1 **To what extent is compliance with information security ensured in procedures and processes?**
Do jaké míry je v postupech a procesech zajištěn soulad s informační bezpečností?
Nestačí definovat požadavky na bezpečnost informací a připravit a zveřejnit zásady. Je důležité pravidelně kontrolovat jejich účinnost.

1.5.2 **To what extent is the ISMS reviewed by an independent authority?**
Do jaké míry je ISMS přezkoumáván nezávislou autoritou?
Posuzování účinnosti ISMS pouze z interního hlediska je jako základní kontrolní mechanismus nedostatečné. Kromě toho bude v pravidelných intervalech a v případě zásadních změn prováděno nezávislé, a tudíž objektivní hodnocení.

1.6 Incident and Crisis Management

1.6.1 **To what extent are information security relevant events or observations reported?**
Do jaké míry jsou hlášeny incidenty nebo události související s bezpečností informací? Potenciální bezpečnostní události nebo pozorování zjistí kdokoli. Je životně důležité, aby kdokoli mohl a věděl, kdy a jak nahlásit vše, co pozoroval a co má potenciální bezpečnostní důsledky (pozorování) nebo události, aby se odborníci mohli rozhodnout, zda a jak je třeba s tím naložit.

1.6.2 **To what extent are reported security events managed?** **New 6.0**
Do jaké míry jsou řízeny hlášené bezpečnostní incidenty?
Jakmile jsou nahlášeny bezpečnostní události, je životně důležité, aby bylo řízení událostí řízeno. To znamená zajistit, že typ a závažnost nahlášené události, stejně jako odpovědné osoby, budou rychle identifikovány, aby bylo zajištěno, že časově kritické aspekty lze zvládnout včas. Jakmile je identifikace provedena, je nutné zajistit, aby se odpovědné osoby dozvěděly a vypořádaly se s událostí v přiměřeném časovém rámci. Kromě toho, pokud se událost týká více různých osob, nebo řízení zahrnuje také koordinaci komunikace, je důležitou součástí řízení události. A konečně, pokud existují externí (smluvní nebo regulační) požadavky na podávání zpráv, je důležité zajistit, aby byly splněny také profesionálním způsobem.

1.6 Incident and Crisis Management

1.6.3 **To what extent is the organization prepared to handle crisis situations? VDA 6.0**

Do jaké míry je organizace připravena řešit krizové situace?

Nastane krizová situace Pokud výjimečné situace (např. přírodní katastrofy, fyzické útoky, pandemie, výjimečné sociální situace, kybernetické útoky způsobující velká selhání infrastruktury) vážně narušují klíčové obchodní operace. V takových případech je hlavní prioritou organizace zvládnout situaci co nejšetrněji a co nejrychleji se zotavit. Abychom toho dosáhli, a protože čas je zásadní, je obvyklým přístupem přechod na režim krizového řízení, který provádí předem naplánované postupy se specifickým rozdělením odpovědností a struktur, umožňuje organizaci se s takovou situací vypořádat.

2 Human Resources

2.1.1 **To what extent is the qualification of employees for sensitive work fields ensured?**

Do jaké míry je zajištěna kvalifikace zaměstnanců pro citlivé pracovní role?

Kompetentní, spolehliví a důvěryhodní zaměstnanci jsou klíčem k informační bezpečnosti v rámci organizace. Proto je důležité prověřovat kvalifikaci potenciálních zaměstnanců (např. uchazečů) v odpovídající míře.

2.1.2 **To what extent is all staff contractually bound to comply with information security policies?**

Do jaké míry jsou všichni zaměstnanci smluvně zavázáni dodržovat zásady bezpečnosti informací?

Organizace podléhají legislativě, nařízením a vnitřním zásadám. Již při najímání zaměstnanců je třeba zajistit, aby se zaměstnanci zavázali k dodržování zásad a byli si vědomi důsledků nesprávného jednání.

2 Human Resources

2.1.3 **To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?**

Do jaké míry jsou zaměstnanci informováni a proškoleni s ohledem na rizika vyplývající z nakládání s informacemi?

Pokud nejsou zaměstnancům známy požadavky a rizika informační bezpečnosti, existuje riziko pochybení vedoucí k poškození organizace. Proto je důležité, aby informační bezpečnost byla internalizována (vnitřně osvojuje) a praktikována jako přirozená součást jejich práce.

2.1.4 **To what extent is mobile work regulated?**

Do jaké míry je mobilní práce regulována?

Práce mimo specificky definované bezpečnostní zóny (home office/ teleworking) vytváří rizika vyžadující odpovídající ochranná opatření.

3 Physical Security

3.1.1 **To what extent are security zones managed to protect information assets?**
Do jaké míry jsou bezpečnostní zóny spravovány pro ochranu informačních aktiv?
Bezpečnostní zóny poskytují fyzickou ochranu informačních aktiv. Čím citlivější jsou informační aktiva, která mají být zpracována, tím více ochranných opatření jsou vyžadována.

3.1.2 **To what extent is information security ensured in exceptional situations? VDA 5.1**
Do jaké míry je zajištěna informační bezpečnost ve výjimečných situacích? Exceptional situations (e.g. natural disasters, physical attacks, cyber attacks, exceptional social situations, incidents or infrastructure failures of significant impact) present a great challenge to the organization. Good preparation helps to ensure that information security risks are adequately considered even in exceptional situations.
Výjimečné situace (např. přírodní katastrofy, fyzické útoky, kybernetické útoky, výjimečné sociální situace, incidenty nebo selhání infrastruktury s významným dopadem) představují pro organizaci velkou výzvu. Dobrá příprava pomáhá zajistit, aby rizika informační bezpečnosti byla adekvátně zvážena i ve výjimečných situacích.

3.1.2 n/a **Superseded by 1.6.3, 5.2.8 and 5.2.9 VDA ISA 6.0**
Nahrazeno 1.6.3, 5.2.8 a 5.2.9

3 Physical Security

3.1.3 **To what extent is the handling of supporting assets managed?**

Do jaké míry je spravováno nakládání s podpůrným majetkem?

Během svého životního cyklu (např. používání, likvidace) jsou podpůrná aktiva vystavena rizikům, jako je ztráta, krádež nebo neoprávněné prohlížení.

3.1.4 **To what extent is the handling of mobile IT devices and mobile data storage devices managed?**

Do jaké míry je řízena manipulace s mobilními IT zařízeními a mob. datovými úložišti?

Mobilní IT zařízení (např. notebooky, tablety, smartphony) a mobilní datová úložiště (např. SD karty, pevné disky) se obecně používají nejen v prostorách organizace, ale také v mobilních aplikacích. To představuje zvýšené riziko s ohledem např. ztráta nebo krádež.

4 Identity and Access Management

4.1 Identity Management

4.1.1 **To what extent is the use of identification means managed?**

Do jaké míry je řízeno používání identifikačních prostředků?

Ke kontrole autorizace pro fyzický i elektronický přístup se často používají prostředky identifikace, jako jsou klíče, vizuální ID, další zařízení pro fyzický přístup a také kryptografické tokeny. Bezpečnostní prvky jsou spolehlivé pouze tehdy, pokud je použití takových identifikačních prostředků adekvátně řešeno.

4.1.2 **To what extent is the user access to IT services and IT systems secured?**

Do jaké míry je zabezpečen přístup uživatelů k IT službám a IT systémům?

Přístup do IT systémů mají získat pouze bezpečně identifikovaní (ověření) uživatelé. Za tímto účelem je totožnost uživatele bezpečně určena vhodnými postupy.

4.1.3 **To what extent are user accounts and login information securely managed and applied?**

Do jaké míry jsou uživatelské účty a přihlašovací údaje bezpečně spravovány a používány?

Přístup k informacím a IT systémům je poskytován prostřednictvím ověřených uživatelských účtů přiřazených osobě. Je důležité chránit přihlašovací údaje a zajistit sledovatelnost transakcí a přístupů.

4 Identity and Access Management
4.2 Access Management

4.2.1 **To what extent are access rights assigned and managed?**

Do jaké míry jsou přidělována a spravována přístupová práva?

Správa přístupových práv zajišťuje, že k informacím a IT službám mají přístup pouze oprávnění uživatelé. Za tímto účelem jsou uživatelským účtům přidělena přístupová práva.

NIS2 - Správa a ověřování identit § 20

- Použití hesel je pouze **poslední** a **dočasná** možnost!
- Min. požadavky na hesla
  - Uživatel 12 znaků
  - Admin 17 znaků
  - Technická aktiva 22 znaků
  - Možnost 64 znaků
  - Možnost všech typů znaků
  - Změna po 30 min
  - Povinná změna po 18 měsícíc
- **MFA** jako základ
  - Jinak evidence výjimky a **klíče/certifikáty**
    - Jinak v nástroji **ID a heslo**
- **Nástroj** pro správu a ověření identity (admina, uživatele technického aktiva) – adresářové služby, např. MS AD, RADIUS, OpenLDAP, apod.
  - Ověření identity
  - Řízení počtu neúspěšných pokusů o přihlášení
  - Zabezpečení údajů
  - Znovu ověření po nečinnosti
  - Bezpečné předání výchozích údajů (náhodné, hned změna, zneplatnění po 24 hod)
  - Centralizovaná správa

5 IT Security / Cyber Security

5.1 Cryptography

5.1.1 **To what extent is the use of cryptographic procedures managed?**

Do jaké míry je řízeno používání kryptografických postupů?

Při používání kryptografických postupů je důležité zvážit rizika v oblasti dostupnosti (ztráta klíčového materiálu) i rizika způsobená nesprávně aplikovanými postupy v oblasti integrity a důvěrnosti (špatné algoritmy/protokoly nebo nedostatečná síla klíče).

5.1.2 **To what extent is information protected during transfer?**

Do jaké míry jsou informace během přenosu chráněny?

Při přenosu prostřednictvím veřejných nebo soukromých sítí mohou být informace za určitých okolností čteny nebo s nimi manipulovány neoprávněnými třetími stranami. Proto musí být stanoveny a implementovány požadavky týkající se potřeby ochrany informací přijetím vhodných opatření během takového přenosu.

5 IT Security / Cyber Security
5.2 Operations Security

5.2.1 **To what extent are changes managed?**
Do jaké míry jsou změny řízeny?
Cílem je zajistit zohlednění aspektů informační bezpečnosti v případě jakýchkoli změn v organizaci, obchodních procesech a IT systémech (Change Management), aby tyto změny nezpůsobily nekontrolované snížení úrovně bezpečnosti informací.

5.2.2 **To what extent are development and testing environments separated from operational environments?**
Do jaké míry jsou vývojová a testovací prostředí oddělena od provozních?
Cílem oddělení vývojového, testovacího a provozního prostředí je zajistit zachování dostupnosti, důvěrnosti a integrity produktivních dat.

5.2.3 **To what extent are IT systems protected against malware?**
Do jaké míry jsou IT systémy chráněny proti malwaru?
Cílem je technicky i organizačně zajistit ochranu IT systémů před malwarem.

5 IT Security / Cyber Security
5.2 Operations Security

5.2.4 **To what extent are event logs recorded and analysed?**
Do jaké míry jsou logy událostí zaznamenávány a analyzovány?
Protokoly událostí podporují sledovatelnost událostí v případě bezpečnostního incidentu. To vyžaduje, aby události nezbytné k určení příčin byly zaznamenány a uloženy. Kromě toho je nutné protokolování a analýza činností v souladu s platnou legislativou (např. zákon o ochraně osobních údajů nebo zákoník práce), aby bylo možné určit, který uživatelský účet provedl změny v systémech IT.

NIS2 - Logování § 23 - Požadované minimální typy logovaných událostí – min. 18 měsíců

- Přihlašování/odhlašování
- Privilegované činnosti (i neúspěšný pokus)
- Manipulace s oprávněními (i neúspěšný pokus)
- Zahájení/ukončení činnosti technických aktiv
- Kritická chybová hlášení technických aktiv
- Přístup k záznamům událostí a pokus o změnu
- Další činnosti – plyne např. z analýzy rizik

5 IT Security / Cyber Security
5.2 Operations Security

5.2.5 **To what extent are vulnerabilities identified and addressed?**

Do jaké míry jsou zranitelná místa identifikována a řešena?

Zranitelnosti zvyšují riziko, že IT systémy nebudou schopny splnit požadavky na důvěrnost, dostupnost a integritu. Využití zranitelností patří mezi možné způsoby, jak mohou útočníci získat přístup k IT systému nebo ohrozit jeho provozní stabilitu.

5.2.6 **To what extent are IT systems and services tech checked (system and service audit?**

Do jaké míry jsou IT systémy a služby technicky kontrolovány (systém. a servisní audit)?

Cílem technických kontrol je odhalování stavů, které mohou ohrozit dostupnost, důvěrnost nebo integritu IT systémů a služeb.

NIS2 – Aplikační bezpečnost § 25

- Používat pouze podporovaná technická aktiva a všechny aktualizace – jinak **Evidence** a **Bezpečnostní opatření**
- Pravidelné **skenování zranitelností** min. 1x/rok (z interní a externí sítě),

  Následně zhodnocení rizik a opatření
- **Penetrační testování** dle rizik min. 1x/2 roky
  - Před uvedením do provozu
  - Při významné změně

  Následně hodnocení rizik, opatření a **retest**

5 IT Security / Cyber Security
5.2 Operations Security

5.2.7 **To what extent is the network of the organization managed?**
Do jaké míry je spravována síť organizace?
IT systémy v síti jsou vystaveny různým rizikům nebo mají různé potřeby ochrany. Aby bylo možné odhalit nebo zabránit nechtěné výměně dat nebo přístupu mezi těmito IT systémy, jsou tyto systémy rozděleny do vhodných segmentů a přístup je řízen a monitorován pomocí bezpečnostních technologií.

NIS2 – Vyhodnocování kybernetických bezpečnostních událostí § 22

- **Nástroj** pro vyhodnocování kybernetických bezpečnostních událostí
  - SIEM (Security Information and Event Management)
  - Schopnost kombinovat informace z více zdrojů (např. uživatel neprošel vstupním turniketem, ale přihlásil se na počítači v objektu, apod.)
- **Aktualizovat** nastavení nástroje, užitých pravidel a alertingu
  (**nekonečný proces**, nastavení musí odpovídat měnícím se potřebám)

5 IT Security / Cyber Security
5.2 Operations Security

5.2.8 **To what extent is continuity planning for IT services in place? VDA 6.0**
Do jaké míry je zavedeno plánování kontinuity pro IT služby?
Plánování kontinuity (včetně pohotovostních) pro IT služby je součástí celkového programu pro dosažení kontinuity operací pro organizační poslání a důležité obchodní funkce. Akce řešené v plánech kontinuity zahrnují řádnou degradaci systému, vypnutí systému, návrat do manuálního režimu, alternativní toky informací a provoz v režimech vyhrazených pro případ výskytu bezpečnostního incidentu.

5.2.9 **To what extent is the backup and recovery of data and IT services ensured? VDA 6.0**
Do jaké míry je zajištěno zálohování a obnova dat a IT služeb?
Data a služby IT se mohou stát nedostupnými v důsledku událostí, jako jsou selhání hardwaru, závady SW, chyby operátora nebo útoky. Zálohování a obnova umožňuje organizacím zotavit se z relevantních situací a omezit potenciální poškození organizace na rozumnou částku.

5 IT Security / Cyber Security
5.3 System acquisitions, requirement management and development

5.3.1 **To what extent is inf. security considered in new or further developed IT systems?**
Do jaké míry je inf. bezp. zohledňována v nových nebo dále vyvíjených IT systémech?
Informační bezpečnost je nedílnou součástí celého životního cyklu IT systémů. To zahrnuje zejména zohlednění požadavků na informační bezpečnost při vývoji nebo akvizici IT systémů.

5.3.2 **To what extent are requirements for network services defined?**
Do jaké míry jsou definovány požadavky na síťové služby?
Síťové služby mají různé požadavky na informační bezpečnost, kvalitu přenosu dat nebo správu. Je důležité znát tato kritéria a rozsah použití různých síťových služeb.

5.3.3 **To what extent is the return and secure removal of information assets from external IT services regulated?**
Do jaké míry je regulováno vracení a bezpečné odstraňování informačních aktiv z externích IT služeb?
Aby byla jako vlastník informací zajištěna kontrola nad informačními aktivy, je nutné, aby informační aktiva mohla být bezpečně odstraněna nebo byla v případě potřeby vrácena při ukončení IT služby.

5 IT Security / Cyber Security

5.3 System acquisitions, requirement management and development

5.3.4 **To what extent is information protected in shared external IT services?**

Do jaké míry jsou informace chráněny ve sdílených externích IT službách?

Musí být zajištěna jasná segregace mezi jednotlivými klienty tak, aby byly vždy chráněny vlastní informace v externích IT službách a aby k nim neměly přístup jiné organizace (klienti).

6 Supplier Relationships

6.1.1 **To what extent is information security ensured among contractors and cooperation partners?**
„Do jaké míry je zajištěna informační bezpečnost mezi dodavateli a kooperačními partnery?
Při spolupráci s kooperačními partnery a dodavateli je rovněž udržována odpovídající úroveň informační bezpečnosti.

6.1.2 **To what extent is non-disclosure regarding the exchange of information contractually agreed?**
Do jaké míry je mlčenlivost ohledně výměny informací smluvně dohodnuta?
Dohody o mlčenlivosti poskytují právní ochranu informací organizace, zejména tam, kde dochází k výměně informací za hranicemi organizace.

7 Compliance

7.1.1 **To what extent is compliance with regulatory and contractual provisions ensured?**

Do jaké míry je zajištěn soulad s regulačními a smluvními ustanoveními?

Nedodržení právních, regulačních nebo smluvních ustanovení může představovat rizika pro informační bezpečnost zákazníků a vlastní organizace. Proto je nezbytné zajistit, aby tato ustanovení byla známa a dodržována.

7.1.2 **To what extent is the protection of personally identifiable data considered when implementing information security?**

Do jaké míry je při zavádění informační bezpečnosti zvažována ochrana osobních údajů?

Soukromí a ochrana osobních údajů jsou zohledňovány při implementaci informační bezpečnosti, jak to vyžadují příslušné národní zákony a předpisy, kde je to vhodné.

8 Prototype Protection

Prototypová ochrana chrání fyzické prototypy, které jsou klasifikovány jako vyžadující ochranu. Prototypy zahrnují vozidla, komponenty a díly. Vlastník duševního vlastnictví k prototypu je považován za vlastníka prototypu.
Za klasifikaci potřeby ochrany prototypu je odpovědné oddělení uvádění do provozu majitele. Pro prototypy klasifikované jako vyžadující vysokou nebo velmi vysokou ochranu musí být uplatněny minimální požadavky na ochranu prototypu.

8.1 Physical and Environmental Security

Fyzická prostředí a bezpečnost prostředí

Požadavky popsané v této části platí pro všechny společnosti, které na základě svých vlastních vlastností vyrábějí, skladují nebo poskytují k použití vozidla, součásti nebo díly klasifikované jako vyžadující ochranu.

8.1.1 **To what extent is a security concept available describing minimum requirements regarding the physical and environmental security for prototype protection?**

Do jaké míry je k dispozici bezpečnostní koncept popisující minimální požadavky na fyzickou a environmentální bezpečnost pro ochranu prototypů?

Nezbytná opatření pro ochranu prototypů musí být aplikována a implementována na vlastnosti a zařízení dodavatelů, vývojových partnerů a poskytovatelů služeb. Bezpečnostní koncept musí stanovit příslušný provozovatel. Realizace a dodržování opatření fyzické a environmentální bezpečnosti definovaných v bezpečnostní koncepci musí zajistit odpovědný provozovatel.

8 Prototype Protection

8.1 Physical and Environmental Security

8.1.2 **To what extent is perimeter security existent preventing unauthorized access to protected property objects?**

Do jaké míry existuje zabezpečení perimetru, které brání neoprávněnému přístupu k objektům chráněného majetku?

Musí být zabráněno neoprávněnému přístupu k nemovitostem, kde jsou vyráběna, zpracovávána nebo skladována vozidla, součásti nebo díly klasifikované jako vyžadující ochranu.

8.1.3 **To what extent is the outer skin of the protected buildings constructed such as to prevent removal or opening of outer-skin components using standard tools?**

Do jaké míry je vnější plášť chráněných budov konstruován tak, aby zabránil odstranění nebo otevření součástí vnějšího pláště pomocí standardních nástrojů?

Musí být zabráněno neoprávněnému přístupu do budov/bezpečnostních oblastí, kde se vyrábějí, zpracovávají nebo skladují vozidla, součásti nebo díly klasifikované jako vyžadující ochranu.

8.1.4 **To what extent is view and sight protection ensured in defined security areas?**

Do jaké míry je zajištěna ochrana zraku a zraku ve vymezených bezpečnostních oblastech?

Musí být zajištěno, aby bylo zabráněno neoprávněnému prohlížení vozidel, součástí nebo dílů klasifikovaných jako vyžadující ochranu.

8 Prototype Protection

8.1 Physical and Environmental Security

8.1.5 **To what extent is the protection against unauthorized entry regulated in the form of access control?**
Do jaké míry je upravena ochrana před neoprávněným vstupem formou kontroly vstupu? Musí být zajištěno, aby všechny přístupové body do bezpečnostních oblastí, kde se vyrábějí, zpracovávají nebo skladují vozidla, součásti nebo díly klasifikované jako vyžadující ochranu, byly chráněny proti neoprávněnému vstupu odpovídajícími opatřeními.

8.1.6 **To what extent are the premises to be secured monitored for intrusion?**
Do jaké míry jsou prostory, které mají být zabezpečeny, monitorovány z hlediska narušení?
Musí být zajištěno, aby prostory, kde se vyrábějí, zpracovávají nebo skladují vozidla, součásti nebo díly klasifikované jako vyžadující ochranu, byly sledovány z hlediska vniknutí. Je zajištěno včasné zpracování alarmu.

8.1.7 **To what extent is a documented visitor management in place?**
Do jaké míry je zaveden dokumentovaný management návštěvnosti?
Ochrana před neoprávněným přístupem do bezpečnostních oblastí, kde jsou vyráběna, zpracovávána nebo skladována vozidla, součásti nebo díly klasifikované jako vyžadující ochranu, včetně sledovatelné dokumentace.

8 Prototype Protection 8.1 Physical and Environmental Security

8.1.5 **To what extent is the protection against unauthor entry regulated in the form ofAC?**

Do jaké míry je upravena ochrana před neoprávněným vstupem formou kontroly vstupu? Musí být zajištěno, aby všechny přístupové body do bezpečnostních oblastí, kde se vyrábějí, zpracovávají nebo skladují vozidla, součásti nebo díly klasifikované jako vyžadující ochranu, byly chráněny proti neoprávněnému vstupu odpovídajícími opatřeními.

8.1.6 **To what extent are the premises to be secured monitored for intrusion?**

Do jaké míry jsou prostory, které mají být zabezpečeny, monit. z hlediska narušení?

Musí být zajištěno, aby prostory, kde se vyrábějí, zpracovávají nebo skladují vozidla, součásti nebo díly klasifikované jako vyžadující ochranu, byly sledovány z hlediska vniknutí. Je zajištěno včasné zpracování alarmu.

8.1.7 **To what extent is a documented visitor management in place?**

Do jaké míry je zaveden dokumentovaný management návštěvnosti?

Ochrana před neoprávněným přístupem do bezpečnostních oblastí, kde jsou vyráběna, zpracovávána nebo skladována vozidla, součásti nebo díly klasifikované jako vyžadující ochranu, včetně sledovatelné dokumentace.

8.1.8 **To what extent is on-site client segregation existent?**

Do jaké míry existuje segregace klientů na místě?

Aby byla vždy zajištěna ochrana specifického know-how klienta, musí být zajištěna jasná segregace klientů. Jedná se zejména o ochranu před neoprávněným prohlížením a přístupem do oblastí, kde se zpracovávají nebo skladují vozidla, komponenty nebo díly.

8 Prototype Protection

8.2 Organizational Requirements

8.2.1 **To what extent are non-disclosure agreements/obligations existent according to the valid contractual law?**

Do jaké míry existují dohody/závazky o mlčenlivosti podle platného smluvního práva?

Při přenosu informací klasifikovaných jako vyžadující ochranu je třeba zajistit, aby externí org. byly povinny plnit požadavky na bezpečnost informací a aby byla provedena související nezbytná opatření. Nezbytný právní základ pro tuto povinnost poskytují dohody o mlčenlivosti. Proto je třeba zajistit, aby informace klasifikované jako vyžadující ochranu byly předávány pouze tehdy, pokud byla uzavřena taková dohoda o mlčenliv. a je právně účinná.

8.2.2 **To what extent are requirements for commissioning subcontr. known and fulfilled?**

Do jaké míry jsou známy a splněny požadavky na uvedení subdodavatelů do provozu? Při zapojení subdodavatelů musí být splněny minimální požadavky na ochranu prototypu.

8.2.3 **To what extent do employees and project members evidently participate in training and awareness measures regarding the handling of prototypes?**

Do jaké míry se zaměstnanci a členové projektu evidentně podílejí na školeních a osvětových opatřeních týkajících se zacházení s prototypy?

Na školeních/osvětových seminářích na téma ochrana prototypů musí zaměstnanci získat potřebné znalosti a dovednosti pro bezpečné zacházení s vozidly, součástmi a díly klasifikovanými jako vyžadující ochranu.

8 Prototype Protection
8.2 Organizational Requirements

8.2.4 **To what extent are security classifications of the project and the resulting security measures known?**
Do jaké míry jsou známy bezp. klasifikace projektu a z toho vyplývající bezp. opatření?
Musí být zajištěno, že bezpečnostní klasifikace a požadavky ve vztahu k postupu projektu jsou známy a dodržovány každým členem projektu.

8.2.5 **To what extent is a process defined for granting access to security areas?**
Do jaké míry je definován proces udělování přístupu do bezpečnostních oblastí?
Proces je definován pro ochranu před neoprávněným přístupem do bezpečnostních oblastí, kde jsou vyráběna, zpracovávána nebo skladována vozidla, komponenty nebo díly klasifikované jako vyžadující ochranu.

8 Prototype Protection
8.2 Organizational Requirements

8.2.6 **To what extent are regulations for image recording and handling of created image material existent?**
Do jaké míry existují předpisy pro záznam obrazu a manipulaci s vytvořeným obraz. mat.?
Musí být definovány předpisy pro záznam snímků vozidel, součástí nebo dílů klasifikovaných jako vyžadující ochranu, aby se zabránilo neoprávněnému vytvoření nebo přenosu takového obrazového materiálu.

8.2.7 **To what extent is a process for carrying along and using mobile video and photography devices in(to) defined security areas established?**
Do jaké míry je zaveden proces pro přenášení a používání mobilních video a fotografických zařízení v (do) definovaných bezpečnostních oblastech?
Proces je definován pro přenášení a používání mobilních video a fotografických zařízení v (do) bezpečnostních oblastech, kde se vyrábějí, zpracovávají nebo skladují vozidla, součásti nebo díly klasifikované jako vyžadující ochranu. Je třeba zabránit neoprávněnému vytváření nebo přenosu obrazového materiálu.

8 Prototype Protection

8.3 Handling of vehicles, components, and parts

Manipulace s vozidly, komponenty a díly

Během přepravy musí být vozidla, součásti a díly klasifikované jako vyžadující ochranu chráněny před neoprávněným prohlížením, neoprávněným záznamem obrazu a přístupem.
Vozidla, součásti a díly klasifikované jako vyžadující ochranu musí být při parkování/skladování chráněny proti neoprávněnému prohlížení, neoprávněnému fotografování a přístupu.

8.4 Requirements for trial vehicles

Požadavky na zkušební vozidla

Je popsán a implementován proces pro získání specifických požadavků zákazníka na manipulaci s testovacími vozidly klasifikovanými jako vyžadující ochranu. Požadavky popsané v této kapitole se nevztahují na součásti a díly.

8.5 Requirements for events and shootings

Požadavky na akce a natáčení

Požadavky na zabezpečení specifické pro zákazníka pro akce a natáčení týkající se vozidel, součástek nebo dílů klasifikovaných jako vyžadující ochranu jsou známy každému členu projektu. To musí prokázat každá společnost pověřená plánováním, přípravou nebo prováděním akcí nebo natáčení.

Děkuji za pozornost

Ing. Martin Drastich MBA, Ph.D.
604 857 854
Drastich@tuev-nord.cz