SKUPAJ USTVARJAMO IDENTITETO.

Vse, kar je vaš revizor vedno želel vedeti o IAM*

(*in si vas tudi upal vprašati)

BOŠTJAN KOLAR,
pooblaščenec za varnost in skladnost

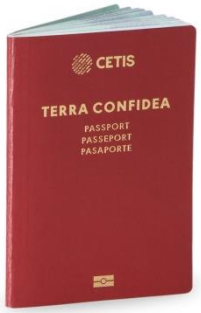
PREDSTAVITEV SKUPINE CETIS

STRATEŠKI EVROPSKI PARTNER NA PODROČJU REŠITEV VARNOSTNIH IN KOMERCIALNIH TISKOVIN

- Število zaposlenih: 583 (Skupina CETIS, 2017)
  - na lokaciji v Celju je cca. 400 zaposlenih (CETIS, CETIS-GRAF, AMBA)
- Prihodki: 61 milijonov evrov (Skupina CETIS, 2017)
- Strateški razvojni partner in ponudnik

VEČ KOT 200 LET IZKUŠENJ NA PODROČJU TISKA

REŠITVE VARNOSTNIH TISKOVIN



CE TRAVEL

- **Biometrični potni listi**
- **Podatkovna stran**
- **Vizumi in sistem najave vizuma od prihodu**
- Zajem podatkov
- Upravljanje podatkov
- AFIS
- Personalizacijske rešitve
- Infrastruktura javnih ključev (PKI)
- Izdaja dokumentov
- Centralni registri
- Rešitve eUprava

CE IDENTITY

- **Osebni dokumenti**
- **Rojstni list in ostali certifikati civilnega statusa**
- Zajem podatkov
- Upravljanje podatkov
- AFIS
- Personalizacijske rešitve
- Infrastruktura javnih ključev (PKI)
- Izdaja dokumentov
- Centralni registri
- Rešitve eUprava

CE TRAFFIC

- **Vozniška dovoljenja**
- **Prometna dovoljenja**
- **Vinjete in druge varnostne etikete za vozila**
- **Tahografske kartice**
- Zajem podatkov
- Upravljanje podatkov
- Personalizacijske rešitve
- Izdaja dokumentov
- Centralni registri
- Rešitve eUprava

CE CARDS

- **Plačilne kartice**
- **Kartice zvestobe**

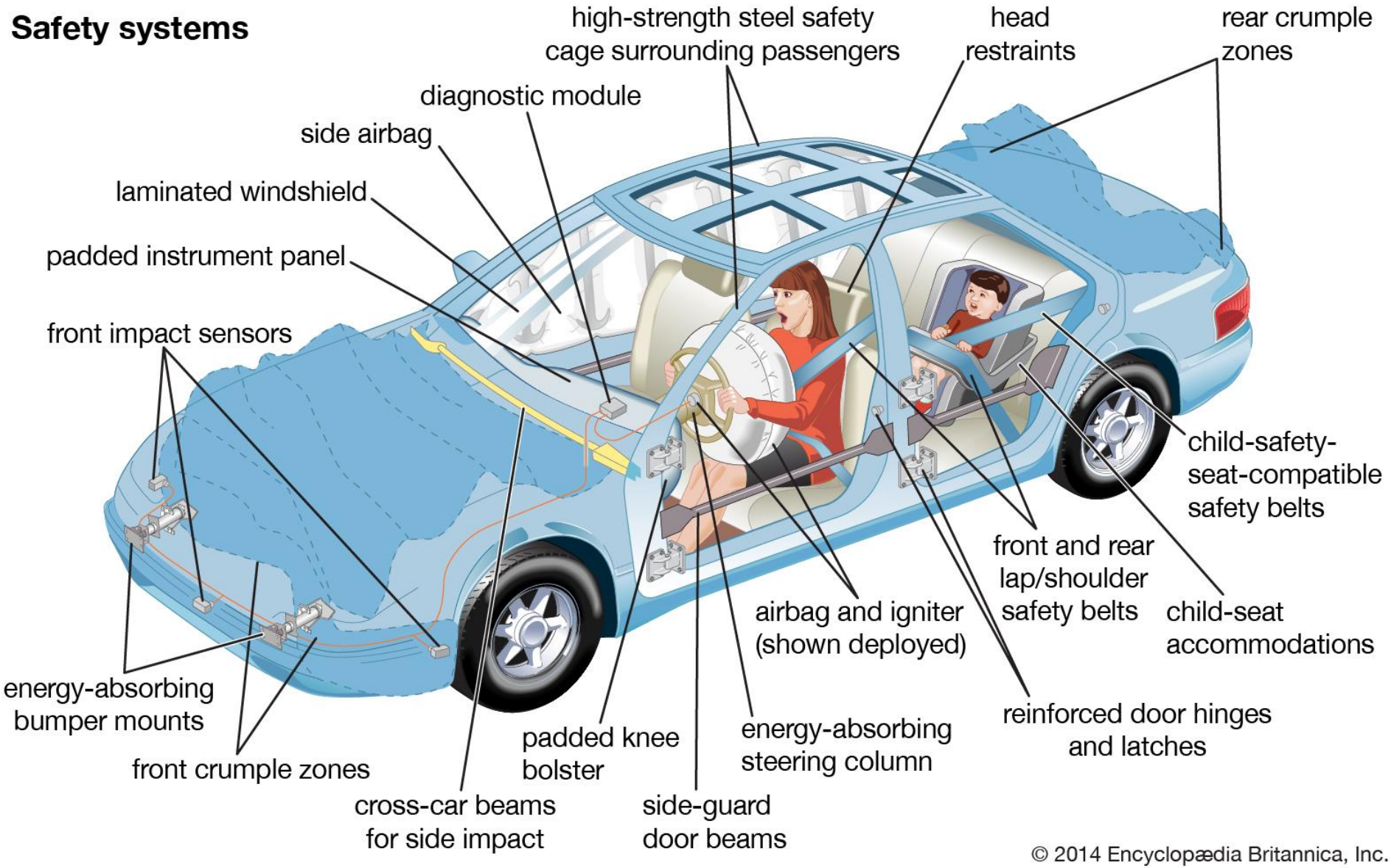
CE SECURE

- **Volilni lističi**
- **Davčne znamke**
- **Varnostne etikete**
- Sistemi sledljivosti

STANDARDI – ZAGOTOVILO KAKOVOSTI

- **ISO 9001** Certificiran sistem vodenja kakovosti.
- **ISO 14001** Certificiran sistem ravnanja z okoljem.
- **ISO 27001** Certificiran sistem upravljanja informacijske varnosti.
- **Certificiran sistem MasterCard/Visa** za zagotavljanje fizične in logične varnosti v skladu z zahtevami PCI (Payment Card Industry).
- Certificiran sistem kakovosti **CQM** (Card Quality Management System) MasterCard za zagotavljanje kakovosti bančnih kartic.
- **FSCC** (Facility Security Clearance Certificate) Varnostno potrdilo vlade Republike Slovenije, Urada za varovanje tajnih podatkov, ki je v skladu z varnostno politiko Evropske unije.
- Certificiran sistem vodenja varovanja za izdelavo visoko varovanih dokumentov **Intergraf ISO 14298 (Central Bank Level)**.
- **DPG** Certifikat Deutsche Pfand Gesellschaft.
- Družba CETIS sledi tudi standardu **ICAO**.

Safety systems



STANDARDI, REGULATIVE, …

ISO 27001

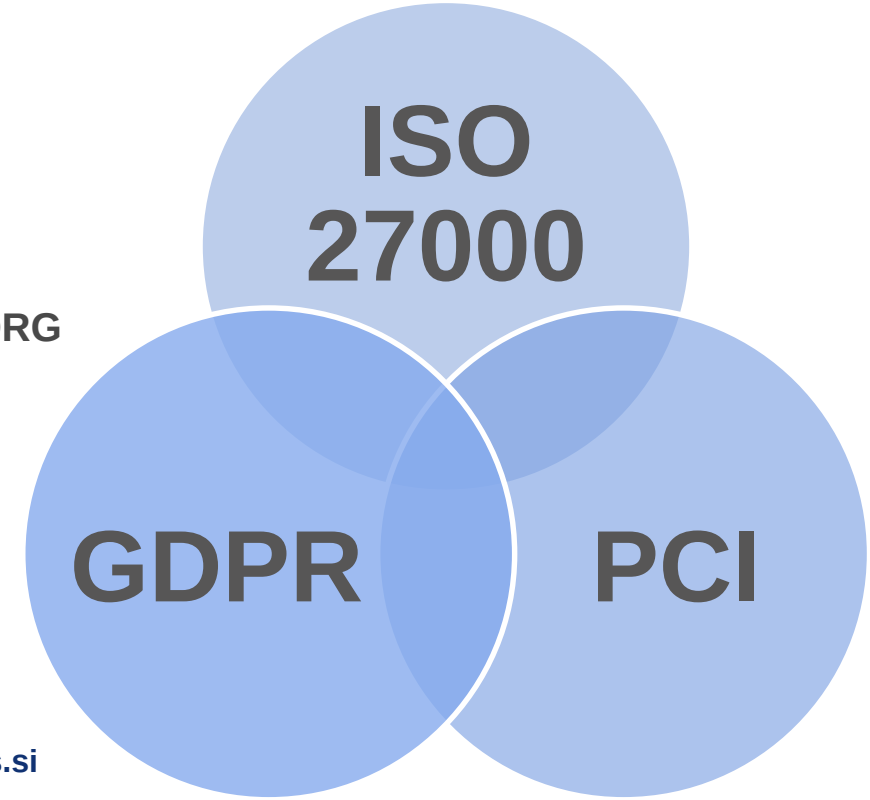
- Najbolj znan svetovni standard upravljanja informacijske varnosti
- Vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja informacijske varnosti.
- Dodatek A: cilji kontrol in kontrole
- Nakup na ISO.ORG

PCI

- Payment Card Industry Standard
- Obvezen za vse dejavnike v svetu plačilnih kartic
- Preskriptiven
- Brezplačno na PCISECURITYSTANDARDS.ORG

GDPR

- Zakonodaja
- Varovanje osebnih podatkov
- Brezplačno na EUROPA.EU



SKUPNE ZAHTEVE REGULATIV ZA IAM

1. Unikatni identifikatorji
2. Dosledna odstranitev dostopov
3. Dostopi na podlagi vlog
4. Odobritev dostopov
5. Periodično preverjanje
6. Konflikt interesa / preprečevanje zlorab
7. Redno ocenjevanje tveganj vezano na dostope

UNIKATNI IDENTIFIKATORJI

Točna identifikacija osebe, ki uporablja sistem; prepoved uporabe skupnih dostopov.

ISO 27001 A.9.2.1 Registracija in izbris registracije uporabnika

- Izvesti se mora formalen postopek za registracijo in izbris registracije uporabnika, da se omogoči dodeljevanje pravic dostopa

PCI DSS 8.1.1 & 8.5

- Assign all users a unique ID before allowing them to access system components or cardholder data.
- Do not use group, shared, or generic IDs, passwords, or other authentication methods

GDPR (64)

- Upravljavec bi moral uporabiti vse razumne ukrepe za preverjanje identitete posameznika, na katerega se nanašajo osebni podatki in ki zahteva dostop do podatkov, zlasti v okviru spletnih storitev in spletnih identifikatorjev. Idr.

DOSLEDNA ODSTRANITEV DOSTOPOV

Uporabniških računov ob prenehanju zaposlitve, ob prenehanju sodelovanja ali ob menjavi vloge.

ISO 27001 A.9.2.6 Preklic ali prilagoditev pravic dostopa

- Pravice dostopa vseh zaposlenih in zunanjih uporabnikov do informacij in naprav za obdelavo informacij se morajo odstraniti po prekinitvi njihove zaposlitve, pogodbe ali dogovora oziroma se prilagoditi spremembam.

PCI DSS 8.1.3

- Immediately revoke access for any terminated users.

GDPR (83)

- Za ohranitev varnosti in preprečitev obdelave, ki bi pomenila kršitev te uredbe, bi moral upravljavec ali obdelovalec …. pozornost posvetiti tveganjem, ki jih pomeni obdelava osebnih podatkov, kot so …. nepooblaščeno razkritje ali dostop do osebnih podatkov ….

DOSTOPI NA PODLAGI VLOG

Določitev vlog in pooblastil ter dodelitev le-teh.

ISO 27001 A.6.1.1 Vloge in odgovornosti na področju informacijske varnosti ter A.9.2.3 Upravljanje posebnih pravic dostopa

- Določiti in dodeliti se morajo vse odgovornosti na področju informacijske varnosti.
- Dodelitev in uporaba posebnih pravic dostopa se morata omejiti in nadzorovati.

PCI DSS 7.1.1, 7.1.3, 7.2.2

- Define access needs for each role, including: System components and data resources that each role needs to access for their job function; Level of privilege required (for example, user, administrator, etc.) for accessing resources.
- Assign access based on individual personnel's job classification and function.
- Assignment of privileges to individuals based on job classification and function.

GDPR (83)

- Za ohranitev varnosti in preprečitev obdelave, ki bi pomenila kršitev te uredbe, bi moral upravljavec ali obdelovalec …. pozornost posvetiti tveganjem, ki jih pomeni obdelava osebnih podatkov, kot so …. nepooblaščeno razkritje ali dostop do osebnih podatkov ….

ODOBRITEV DOSTOPOV

Dostope odobrijo samo pooblaščene osebe, dodelitev v vlogo.

ISO 27001 A.9.1.1 Politika nadzora dostopa ter A.9.2.2 Zagotavljanje dostopa uporabnikom

- Vzpostaviti, dokumentirati in pregledovati se mora politika nadzora dostopa, ki temelji na poslovnih zahtevah in zahtevah informacijske varnosti.
- Izvesti se mora formalen proces zagotavljanja dostopa uporabnikom, da se pravice dostopa dodelijo ali prekličejo za vse vrste uporabnikov za vse sisteme in storitve.

PCI DSS 7.1.4, 8.1.2, 12.3.1

- Require documented approval by authorized parties specifying required privileges.
- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- Explicit approval by authorized parties.

GDPR (83)

- Za ohranitev varnosti in preprečitev obdelave, ki bi pomenila kršitev te uredbe, bi moral upravljavec ali obdelovalec …. pozornost posvetiti tveganjem, ki jih pomeni obdelava osebnih podatkov, kot so …. nepooblaščeno razkritje ali dostop do osebnih podatkov ….

PERIODIČNO PREVERJANJE

Periodično preverjanje s strani pooblaščene in informirane osebe.

ISO 27001 A.9.2.5 Pregled uporabniških pravic dostopa

- Lastniki dobrin morajo pregledovati uporabniške pravice dostopa v rednih časovnih presledkih.

PCI Best practice 5.

- Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.

GDPR (§39)

- Naloge pooblaščene osebe za varstvo podatkov … spremljanje skladnosti s to uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in politikami upravljavca ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;

KONFLIKT INTERESA / PREPREČEVANJE ZLORAB

Preprečite pravice++, razmejitev vlog, preprečevanje zlorab IAM.

ISO 27001 A.6.1.2 Razmejitev dolžnosti & A.9.4.1 Omejitev dostopa do informacij

- Nasprotujoče si naloge in področja odgovornosti se morajo razmejiti, da se zmanjšajo možnosti za nepooblaščeno ali nenamerno spreminjanje ali zlorabo dobrin organizacije.
- Dostop do informacij in sistemskih funkcij aplikacij se mora omejiti v skladu s politiko nadzora dostopa.

PCI DSS 7.1.2, 7.1.4

- Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
- Require documented approval by authorized parties specifying required privileges

GDPR (83)

- Za ohranitev varnosti in preprečitev obdelave, ki bi pomenila kršitev te uredbe, bi moral upravljavec ali obdelovalec …. pozornost posvetiti tveganjem, ki jih pomeni obdelava osebnih podatkov, kot so …. nepooblaščeno razkritje ali dostop do osebnih podatkov ….

REDNO OCENJEVANJE TVEGANJ VEZANO NA DOSTOPE

Redno četrtletno, letno – glede na ocene in zahteve – in ob spremembah.

ISO 27001 6.1.2 Ocenjevanje tveganj informacijske varnosti, A.8.2.1 Klasifikacija informacij

- Organizacija mora določiti in uporabiti proces ocenjevanja tveganj informacijske varnosti...
- Informacije se morajo razvrščati glede na zakonske zahteve, vrednost, kritičnost in občutljivost na nepooblaščeno razkritje ali spreminjanje.

PCI 12.2

- Implement a risk-assessment process that: Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), Identifies critical assets, threats, and vulnerabilities, and Results in a formal, documented analysis of risk.

GDPR (§39)

- Naloge pooblaščene osebe za varstvo podatkov … spremljanje skladnosti s to uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in politikami upravljavca ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;

SKUPNE ZAHTEVE REGULATIV ZA IAM

1. Unikatni identifikatorji
2. Dosledna odstranitev dostopov
3. Dostopi na podlagi vlog
4. Odobritev dostopov
5. Periodično preverjanje
6. Konflikt interesa / preprečevanje zlorab
7. Redno ocenjevanje tveganj vezano na dostope


LEFT REARWARD VEHICLE CAMERA
MEDIUM RANGE VEHICLE CAMERA
RIGHT REARWARD VEHICLE CAMERA
MOTION FLOW
LANE LINES
LANE LINES
ROAD FLOW
IN-PATH OBJECTS
ROAD LIGHTS
OBJECTS
ROAD SIGNS

SKUPAJ USTVARJAMO IDENTITETO.

CETIS®

HVALA.

Z veseljem bomo odgovorili na vsa vaša vprašanja.

www.cetis.si