ISO 27001: MED ZAHTEVAMI STANDARDA IN PRAKSO

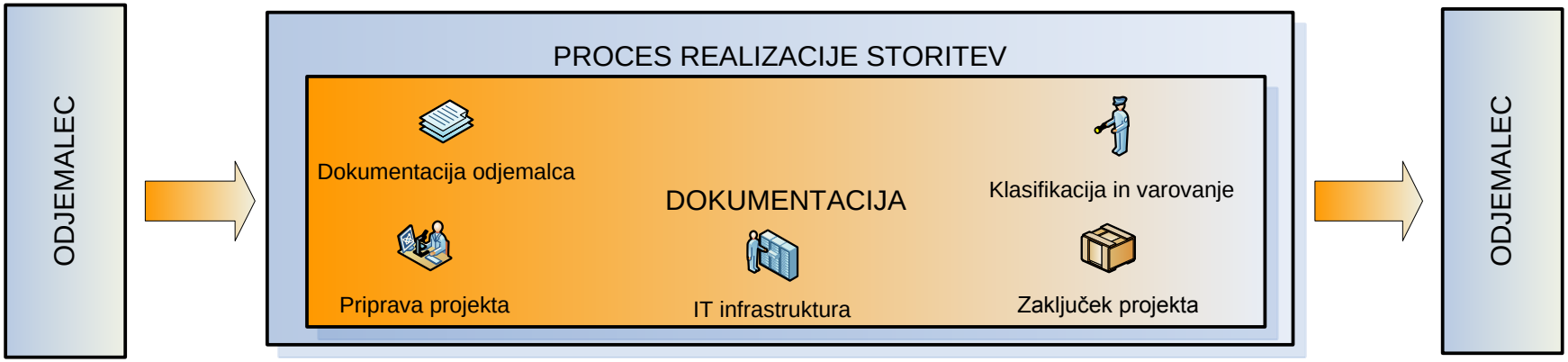
MIHA OZIMEK, SIQ

Stanje varovanja informacij?

Dejansko stanje v organizacijah

- Urejeno poslovanje z ustreznimi varnostnimi kontrolami (dostop, požarna varnost…)
- Informacije in dokumentacija po oddelkih, pisarnah
- Datotečni sistem za hrambo dokumentov v elektronski obliki
- Prevzem vhodne pošte in prenos do zaposlenih
- Elektronska pošta se hrani v elektronskih predalih zavoda ali posameznih zaposlenih…

Analiza aktivnosti organizacije – temelj SUVI



Primer:

Dokumentacija odjemalca: osebni podatki, občutljivi osebni podatki
Podatki o zaposlenih: osebni podatki
Priprava javnih naročil do objave: poslovna skrivnost
Hramba dokumentacije: papirna oblika, elektronska oblika

Kakšna so tveganja? Kakšni so postopki?

Analiza tveganja – proaktivno delovanje

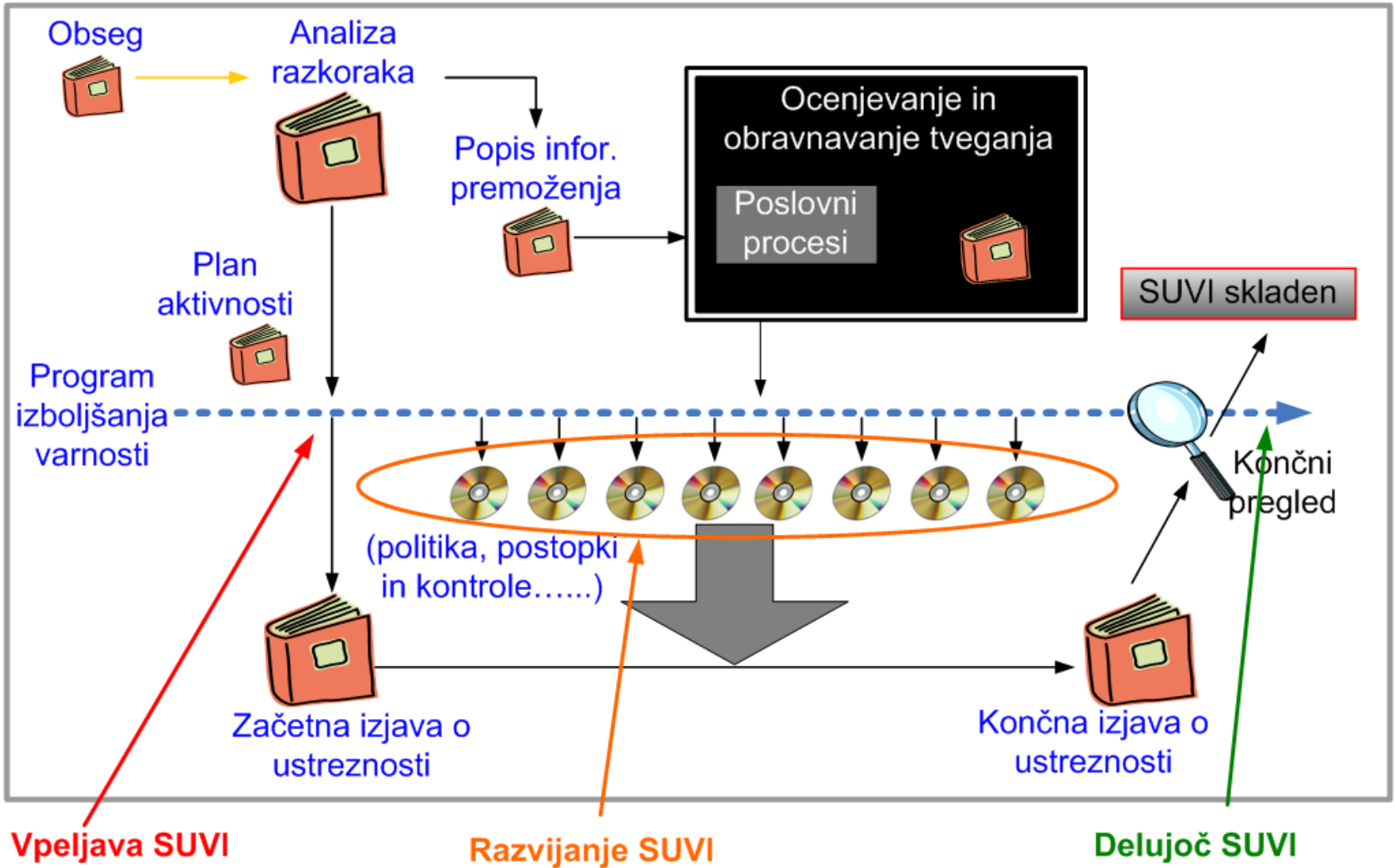
Zbiranje informacij

A) Popis informacijskih sredstev

B) Določitev procesov in zahtev

C) Informacije o uporabljanih varnostnih ukrepih pridobimo iz analize aktivnosti organizacije

Celovito upravljanje z varnostjo



Pravilniki – raziskave in analize

Raziskave in analize		Pravilnik o varstvu osebnih podatkov	Pravilnik o poslovni skrivnosti	Pravila hrambe dok. in arhivskega gradiva
Katere podatke se obvladuje v podjetju?	Podatki	Zbirke OP, vodenje vpogledov…	Dostop do poslovne skrivnosti, vodenje vpogledov…	Dostop do dokumentarnega in arhivskega gradiva…
Kako je postavljeno omrežje, kje se prenašajo podatki?	Omrežje	Pooblaščen dostop	Pooblaščen dostop	Pooblaščen dostop
Kaj uporabljamo za hrambo podatkov?	Strojna oprema	Pooblaščen dostop	Pooblaščen dostop	Pooblaščen dostop
Kaj uporabljamo za hrambo podatkov?	Programska oprema	Revizijske sledi , kriptiranje…	Revizijske sledi , kriptiranje…	Revizijske sledi , kriptiranje…
Kdo so pooblaščene osebe?	Osebje	Izjava o varstvu osebnih podatkov, pooblaščene osebe	Izjava o zaupnosti	Arhivarji
Kakšna je fizična in tehnična zaščita podjetja?	Lokacija, prostori	Zaščita prostorov	Načrt varovanja	Vlaga, temperatura, dostop

- **Enotna pravila za vse sklope podatkov** – ne glede ali so vključeni v hrambo v digitalni obliki ali ne.

- **Klasifikacijski načrt** – vključimo vse podatke organizacije in ga dopolnimo z oznakami glede zaupnosti – točno vemo kako moramo ravnati s posameznim podatkom

- **Enotna pravila za zaposlene** – problem pri postavljanju pravil samo za posamezne sklope podatkov je, da večina zaposlenih pri tem ne bo sodelovala

- **Primerni postopki (ISO 9001) bistveno olajšajo vzpostavitev sistema varovanja informacij!**

- **Politike varovanja informacij (ISO/IEC 27001) moramo vpeljati,** če hočemo pokriti zakonodajne zahteve in določila **– izkoristimo priložnost za vzpostavitev celovitega SUVI!**

- **Vzpostavitev postopkov spremljanja in nadzora** lahko združimo še z spremljanjem kazalnikov uspešnosti organizacije – predstavitev za poslovodstvo!

Kaj prinaša ustrezen način obvladovanja dokumentacije?

- **Klasifikacija** podatkov je enostavna
- **Prenos do pooblaščene osebe je hiter** in manj je stroškov prenašanja dokumentacije
- **Odgovornost** lastnikov/skrbnikov posameznih procesov/delovnih aktivnosti za ustrezni tok dokumentov
- **Dokumenti** se nahajajo na enem mestu
- **Hitro iskanje dokumentov**, iskanje po ustreznih kriterijih

Notranja presoja

Najmanj enkrat letno se izvaja notranje presoje, da ugotovi ali so cilji ukrepov, ukrepi, procesi in postopki glede hrambe dokumentacije:

1. v skladu z zahtevami zakonodaje, pravilnikov / politik / internih aktov,

2. učinkovito vpeljani in vzdrževani.

Vodstveni pregled

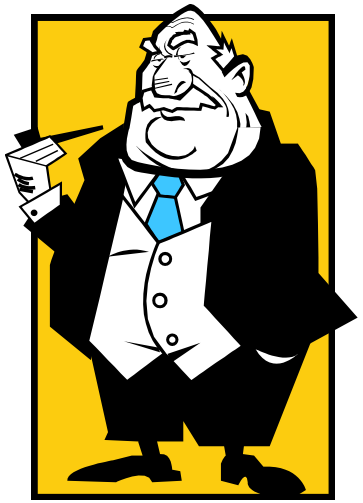
Vodstvo v določenih intervalih pregleduje postopke hrambe

(vsaj 1x letno), da se ugotovi ali je zagotovljena:

- neprekinjena zadostnost
- ustreznost
- učinkovitost hrambe

Ocena možnosti za izboljševanje

Ocena potrebe po spremembah



Kaj prinaša ureditev dokumentacije ter vpeljava SVK in SUVI?

- Prihajajoča zakonodaja se bo primerno upoštevala
- Inšpekcijski pregledi brez težav
- Zaupanje odjemalcev
- Ureditev procesov v organizaciji

Presoje ISO/IEC 27001 - ugotovitve

Pozitivno:

- Zavedanje o zakonodajnih zahtevah glede varstva podatkov
- Primerno reševanje incidentov – hitro, z manj posledicami
- Varnostne kontrole v informacijskih sistemih se postavljajo glede na oceno tveganj

Negativno:

- Preveč kompleksne varnostne politike – niso upoštevane
- Ocena tveganja zaradi presoje – ni delujoč mehanizem
- Incidenti niso razpoznani kot kritični – organizacije se ne zavedajo posredne škode, ki jo prinaša zloraba podatkov

Presoje ISO/IEC 27001 - ugotovitve

Kaj manjka?

- Podpora vodstva marsikje ni dovolj visoka, ker se vodstvo ne zaveda, da brez informacijskega sistema ni možno poslovati.

- SUVI ni samo dokumentiranje varnostnih kontrol ampak vzpostavitev kulture varnosti v organizaciji (če se zavedamo spletnih nevarnosti, je ni primerov incidentov kot so npr. okužbe s kriptovirusi).

- Premalo zavedanja, da morajo tudi zunanje stranke (npr. dobavitelji) biti vključene v SUVI.

Vprašanja?

miha.ozimek@siq.si