ISSR®
SOFTWARE

Znalostná softvérová aplikácia

- manažment incidentov, rizík
- interné audity – postupy
- analýza rizík
- databázy IS, oprávnených osôb
- viacúrovňový prístup, vzory bezpečnostnej dokumentácie
- jednoduché intuitívne ovládanie
- slovenská, česká a anglická verzia
- možnosť vytvárania tlačových zostáv
- nastavovanie systémových užívateľských práv

CYBER SECURITY
BEZPEČNOSŤ INFORMAČNÝCH SYSTÉMOV

1. modul ochrana osobných údajov (podľa ustanovení zákona č. 18/2018 Z. z. o ochrane osobných údajov a Nariadenia Európskeho parlamentu a Rady EÚ 2016/679, „GDPR")

2. modul informačná bezpečnosť (podľa medzinárodného štandardu ISO 27000 a zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.)

Kladiete si nasledovné otázky:

- Čo je to vlastne **informačná bezpečnosť alebo účinná ochrana osobných údajov**, ako ju implementovať v podmienkach našej firmy?
- Je ochrana osobných údajov súčasťou informačnej bezpečnosti alebo len autonómny výmysel na šikanovanie prevádzkovateľov a príležitosť pre právnikov?
- **Vzťahuje sa na nás nová legislatíva**, Nariadenie EP a RADY EÚ č. 2016/679, „GDPR", musíme mať aj u nás vypracované smernice a projekt, máme mať zodpovednú osobu so skúškou na Úrade, resp. DPO, potrebujeme vykonať registrácie IS alebo nemusíme prijať žiadne opatrenia?
- **Ako účinne ochránime osobné údaje fyzických osôb**, aktíva našej firmy?
- Akým spôsobom **predchádzať bezpečnostným incidentom, sankciám zo strany kontrolných orgánov**, ako zautomatizovať a zjednodušiť celý systém ochrany aktív a osobných údajov?
- **Sú nami prijaté opatrenia dostatočné** alebo postačuje prijať ochranné opatrenia len formalizovane?
- Čo je to zostatkové riziko?
- Mám správne identifikované všetky informačné systémy, čo sú to aktíva, analýza rizík?

Pomôžeme Vám s odpoveďami. Jedným z účinných nástrojov je používanie znalostného softvéru ISSR, ktorý Vás prevedie svetom informačnej bezpečnosti a pomôže nastaviť a dlhodobo prevádzkovať funkčný systém ochrany osobných údajov a informačnej bezpečnosti v súlade s legislatívou platnou pre povinné osoby.

Modul ochrana osobných údajov

Čo obsahuje ?

Kompletnú automatizovanú správu riadenia ochrany osobných údajov v organizácii, podľa ustanovení č.18/2018 Z. z. o ochrane osobných údajov a Nariadenia Európskeho parlamentu a Rady EU 2016/679, „GDPR". Ideálny pomocník pre zodpovednú osobu, DPO a oprávnené osoby v organizácii, ktorá vo svojich informačných systémoch spracúva osobné údaje fyzických osôb.

Výhody modulu:

Ak používate tento modul, nemôžete pri ochrane osobných údajov opomenúť žiadnu z podmienok platnej legislatívy a navyše – v systéme udržujete aktualizované informácie v prehľadných databázach. Máte po ruke kompletné prehľady o stave ochrany OÚ, máte informované oprávnené osoby – vhodné pre vstupné interné školenia, predchádzate bezpečnostným incidentom aj oprávnenosti sťažností dotknutých osôb a rovnako sankciám zo strany kontrolnej osoby – výrazne teda šetrí Váš čas a náklady na riešenie bezpečnostných incidentov.

Obsah jednotlivých kapitol:

Kapitola Vzory dokumentácie ochrany osobných údajov

- obsahuje vzory všetkej požadovanej bezpečnostnej dokumentácie – projekt, smernice, poverenia oprávnených osôb, prehlásenia o súhlase a i.

Kapitola Politika ochrany osobných údajov

- obsahuje prehlásenie politiky ochrany osobných údajov v organizácii.

Kapitola Evidencia informačných systémov

- vedie všetky zákonom požadované prvky ochrany osobných údajov: informácie o jednotlivých informačných systémoch (IS) prevádzkovateľa. Ku každému IS vedie informácie požadované zo zákona – označenie, účel spracúvania, právny základ, okruh dotknutých osôb, dátum začiatku spracúvania IS, ďalej vedie údaje o rozsahu osobných údajov spracúvaných v konkrétnom IS, zoznam spracúvaných osobných dokladov, aktuálne zoznamy oprávnených osôb poverených spracúvaním OÚ v konkrétnom IS, zoznam zodpovedných osôb, zoznamy prostriedkov spracúvania, fyzické umiestnenie IS, zoznam sprostredkovateľov k jednotlivým IS, informácie o sprístupňovaní, poskytovaní, zverejňovaní a prenose osobných údajov do tretích krajín, údaje o prevádzkovateľovi IS, vlastnosti IS (evidencia, registrácia, osobitná registrácia, stupeň a popis zabezpečenia IS).

Kapitola Bezpečnostný projekt (Analýza rizík)

- vedie bezpečnostnú dokumentáciu – dokument bezpečnostný projekt . Súčasťou je história a aktuálnosť bezpečnostného projektu
- umožňuje riadený prístup k dokumentu.

Kapitola Bezpečnostné smernice

- vedie bezpečnostnú dokumentáciu – bezpečnostné smernice.
- umožňuje riadený prístup.

Kapitola Zoznam oprávnených a zodpovedných osôb

- vedie databázu oprávnených a zodpovedných osôb a sprostredkovateľov pre jednotlivé IS.

Kapitola Poučenia oprávnených osôb

- vedie bezpečnostnú dokumentáciu – zoznam poučení oprávnených osôb – zamestnancov prevádzkovateľa. Súčasťou je záznam o preškolení oprávnenej osoby. Poučenia sa generujú pre každú oprávnenú osobu individuálne prípadne je možné využiť hromadné generovanie poučení pre viacero oprávnených osôb. Aplikácia umožňuje taktiež nastavovanie povolených činností pre jednotlivé oprávnené osoby a sprostredkovateľov.

Kapitola Incidenty ochrany osobných údajov

- vedie kompletný manažment bezpečnostných incidentov (požadovaný legislatívou) od nahlásenia oprávnenou osobou, popis incidentu, dátumy vzniku, záznamu, text záznamu – popis nápravy – všetky udalosti súvisiace s incidentom.

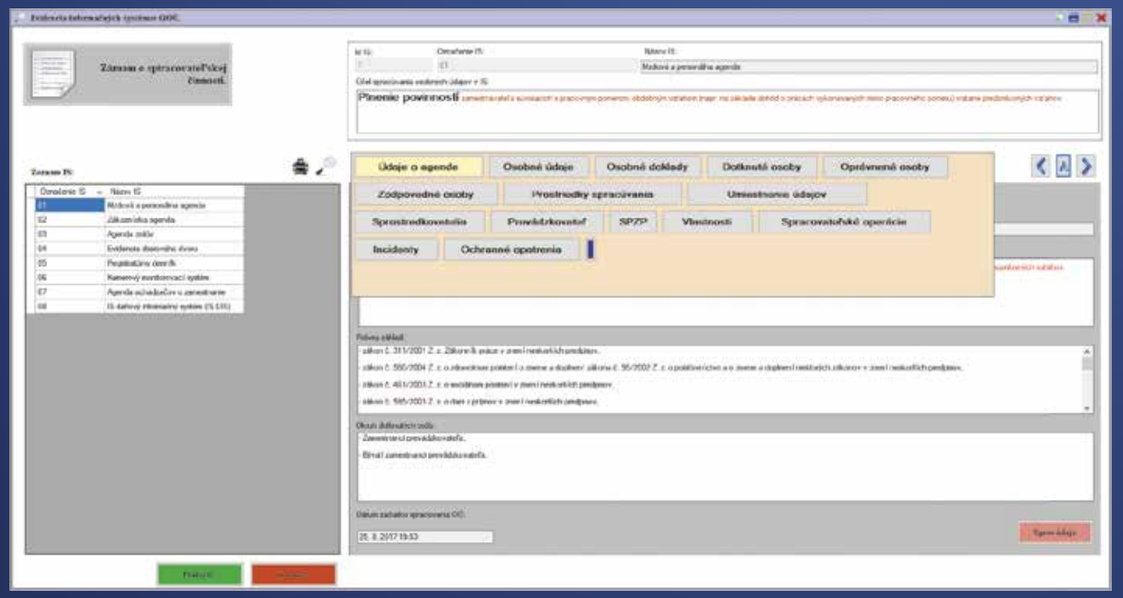
Kapitola Záznamy činností

- vedie podpornú evidenciu – záznamy činností pri ochrane OÚ.

Výhody implementácie softvéru ISSR v module ochrana osobných údajov u prevádzkovateľa:

Softvérová aplikácia ISSR Vám v prípade modulu ochrana osobných údajov poskytne plný komfort riadenia systému ochrany aktíva – osobných údajov fyzických osôb – a to najmä:

- prehľadnosťou prvkov riadenia s detailizáciou podľa ustanovení platnej národnej legislatívy
- zautomatizovaním činností súvisiacich s ochranou osobných údajov
- logickým usporiadaním a viacúrovňovým prístupom , vyhľadáva v databázach, zobrazuje históriu dokumentov (zodpovedná osoba na úrovni administrátora, oprávnené osoby – užívatelia)
- obsahuje podpornú vzorovú dokumentáciu
- manažmentom bezpečnostných incidentov (podmienka požadovaná novou legislatívou)
- databázami s aktualizovanými údajmi v reálnom čase (požadované zákonom aj normami)
- zrýchlením, sprehľadnením práce na dennej báze v organizáciách, pri zmenách fyzického okolia IS, zmenách v IS, aj pri personálnych zmenách oprávnených osôb
- napomáha plniť podmienky dostupnosti, dôvernosti a integrity spracúvaných osobných údajov ako jedného z organizačných opatrení Vašej organizácie
- aplikácia slúži aj ako výborná pomôcka pre zodpovednú osobu pri komunikácii s Úradom na ochranu osobných údajov, pri riešení bezpečnostných incidentov a zároveň pri dennej práci výkonu dohľadu nad ochranou osobných údajov, pri interných školeniach oprávnených osôb, pri výkone interných auditov, rovnako pri vstupných školeniach nových zamestnancov, ktorí budú poverení činnosťou ako oprávnené osoby a poskytuje mnoho ďalších výhod.



ISSR pre bezpečnosť informačných systémov je:

znalostná aplikácia, s lokalizáciou v slovenskom, českom a anglickom jazyku, aplikácia je vytvorená audítormi informačnej bezpečnosti na základe praktických skúseností pri riadení informačnej bezpečnosti a ochrany osobných údajov, vrátane tvorby a udržiavania bezpečnostnej dokumentácie v organizáciách, s pomocou znalostí obsiahnutých v medzinárodných štandardoch a metodikách ISO/IEC, nástrojov riadenia informačnej bezpečnosti, zákonov a metodík národnej legislatívy.

ISSR a legislatíva:

Právny rámec v Slovenskej republike je definovaný zákonom o ochrane osobných údajov č. 18/2018 o ochrane osobných údajov a Nariadenia EP a Rady EÚ 2016/679, „GDPR".
Organizácia (prevádzkovateľ), ktorá spracúva osobné údaje má v zmysle platnej legislatívy povinnosť prijať primerané technické, organizačné a personálne opatrenia na zabezpečenie dôvernosti, dostupnosti a integrity spracúvaných osobných údajov (ďalej len OÚ). Odôvodnenie je uvedené v § 31 zákona č.18/2018 Z. z. o ochrane osobných údajov v Slovenskej republike, resp. § 13 zákona č. 101/2000 Sb. v Českej republike. Príslušná legislatíva taktiež ukladá organizáciám zaoberať sa celkovo problematikou informačnej bezpečnosti, teda nie len z pohľadu ochrany OÚ. To znamená, že požiadavky je potrebné aplikovať na všetky aktíva organizácie, nie len na tie, ktoré sa týkajú OÚ. Ide o celý rad právnych predpisov, opatrení a metodických usmernení, najmä však o zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti. Legislatíva sa v tejto oblasti pravidelne mení, dopĺňa vyhláškami a opatreniami, pričom kopíruje zmeny v oblasti kybernetickej bezpečnosti. Aj z dôvodu týchto aktualizácií je výhodné na riadenie takéhoto zložitého systému používať práve automatizovaný softvér s garantovaným update.

Pre koho je aplikácia určená:

- pre povinné osoby podľa platnej národnej legislatívy
- všetky organizácie, ktoré riadia bezpečnosť informačných systémov a ochranu osobných údajov
- manažérov a štatutárov firiem, manažérov IB, zodpovedné a oprávnené osoby podľa ustanovení zákona č.18/2018 Z. z. o ochrane osobných údajov a Nariadenia Európskeho parlamentu a Rady EU 2016/679, „GDPR", audítorov, odborníkov z oblasti IB.

Je úplne zrejmé, že na procese riadenia IB a OOÚ sa nezúčastňujú len určité vybrané špecifické osoby v organizácii, ale že sa riadenia musia povinne zúčastňovať všetci zamestnanci organizácie. Aby boli teda do dôsledkov naplnené legislatívne požiadavky kladené na povinné osoby, systém riadenia ochrany osobných údajov a kybernetickej bezpečnosti bol plne funkčný a aktívny, minimalizoval sa vznik bezpečnostných incidentov, udržiavala sa dostatočná úroveň bezpečnostného povedomia zamestnancov organizácie, je logickým vyústením konštatovanie, že plnohodnotný prístup k aplikácii ISSR by mali mať všetci zamestnanci organizácie (plné licenčné pokrytie).

Modul informačná bezpečnosť

(zákon č. 69/2018 Z. z., ISO 27000)

Kompletná správa systému riadenia informačnej bezpečnosti

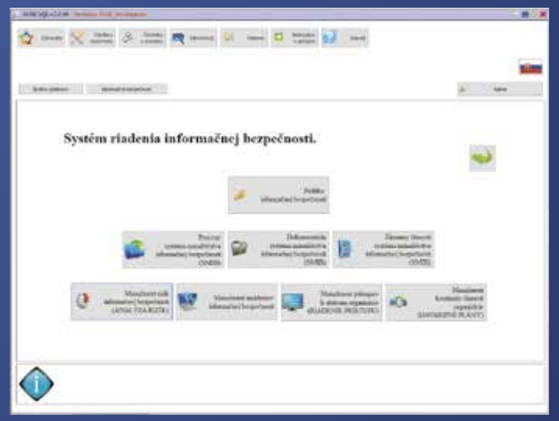
- manažment incidentov, rizík
- interné audity – postupy
- analýza rizík
- databázy prvkov IB
- viacúrovňový prístup

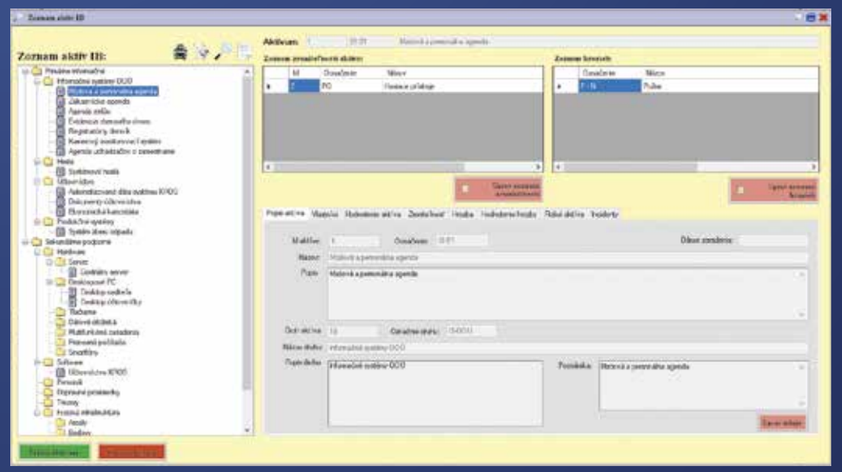
Prečo riadiť bezpečnosť informačných systémov prostredníctvom znalostnej aplikácie?

Základná otázka znie, prečo je potrebné nasadiť sofistikovanú aplikáciu na riadenie informačnej bezpečnosti v organizácii, prečo nestačí len bežné spracovanie agendy vznikajúcej v súvislosti s riadením IB pomocou rôznych dokumentov vydávaných, udržiavaných a revidovaných bežným spôsobom? Čo prinesie nasadenie takejto aplikácie?

Na otázku prečo, možno odpovedať aj protiotázkou: Prečo sa na spracúvanie účtovnej agendy používa sofistikovaný softvér? No preto lebo spracovanie pomocou softvéru prinieslo novú kvalitu, vyššiu úroveň spracúvania a v konečnom dôsledku aj vyššiu produktivitu práce, väčšiu prehľadnosť a pružnosť pri prístupe k výstupom z účtovnej agendy.

Ako to súvisí s riadením IB? Problematika riadenia IB je omnoho zložitejšia ako vedenie účtovnej agendy. Takže nasadenie vhodnej aplikácie na riadenie IB musí priniesť benefity v podobe vyššej kvality a efektivity práce zamestnancov. Keď sa pozrieme detailnejšie na problematiku riadenia IB zistíme, že solídny riadiaci systém so sebou prináša množstvo práce, ktorá vyžaduje vedenie množstva dokumentácie a rôznych záznamov. Len samotný manažment rizík vyžaduje vedenie zoznamov aktív, hrozieb, zraniteľností, dopadov, rizík, ochranných opatrení, atď.. O každom prvku je potrebné viesť určitý druh informácií, jednotlivé prvky sú medzi sebou previazané a tieto informácie je potrebné neustále revidovať a aktualizovať. Jednotlivé prvky IB sú hodnotené, na hodnotení sa podieľa množstvo zamestnancov ich postupy musia byť zdokumentované a preukázateľne verifikované. Udržiavať takýto systém bez nejakého sofistikovaného nástroja je ťažko predstaviteľné.





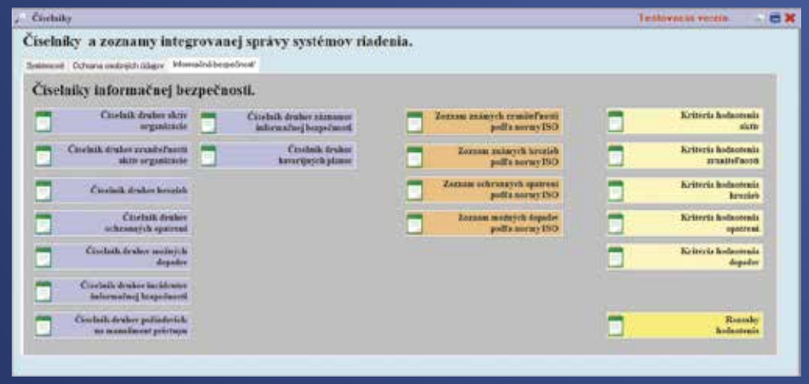
Čo teda prináša aplikácia na riadenie IB:

Správa dokumentácie vznikajúcej v súvislosti s riadením IB (sú to rôzne dokumenty ako politika, manuály, smernice, príkazy, procesy…).
Aplikácia vedie databázu týchto dokumentov a manažuje prístup k nim. Eviduje históriu dokumentu, jeho aktuálnosť, jednoznačne identifikuje vlastníka dokumentu, ktorý zodpovedá za aktuálnosť a platnosť daného dokumentu. Dokumenty sú v štandardnom formáte MS WORD.

Rozsah aplikácie ISSR v module informačná bezpečnosť:

Správa, údržba a vedenie databáz prvkov IB

(Zoznamy aktív, zraniteľností, hrozieb, rizík, zoznam dopadov, zoznam ochranných opatrení.) Súčasťou správy IB je priraďovanie vlastníkov k jednotlivým ochranným opatreniam. Každý zoznam obsahuje informácie potrebné k zabezpečeniu manažmentu rizík. Všetky prvky IB je možné ohodnocovať. Na ohodnocovanie jednotlivých prvkov sa v aplikácii definujú pre každý prvok kritéria hodnotenia, rozsahy hodnotenia a váhy jednotlivých kritérií pri hodnotení daného prvku.



Správa a údržba dokumentov projektu informačnej bezpečnosti v zmysle platnej legislatívy a medzinárodných štandardov
(Vedie zoznam aktuálne platných dokumentov vyžadovaných projektom IB, riadenie revízie a aktualizácie dokumentov projektu IB: politika IB, manuály IB, smernice IB.)

Správa a údržba dokumentácie procesov projektu IB (Procesy návrhu, implementácie, prevádzkovania, monitorovania, preskúmavania, udržiavania a zlepšovania.)

Manažment prevádzkových záznamov vyžadovaný projektom IB
(Vedie databázu záznamov k jednotlivým operáciám, o ktorých sa vyžaduje záznam.)
Databáza záznamov obsahuje minimálne informácie o tom, akej operácie sa tyká, kedy bol záznam vykonaný, kto záznam vykonal.

Manažment rizík, správa a údržba analýz rizík, ANALÝZA RIZÍK
(Zabezpečenie systému hodnotenia aktív, zraniteľností, hrozieb, dopadov a vyhodnocovania úrovne rizika.)

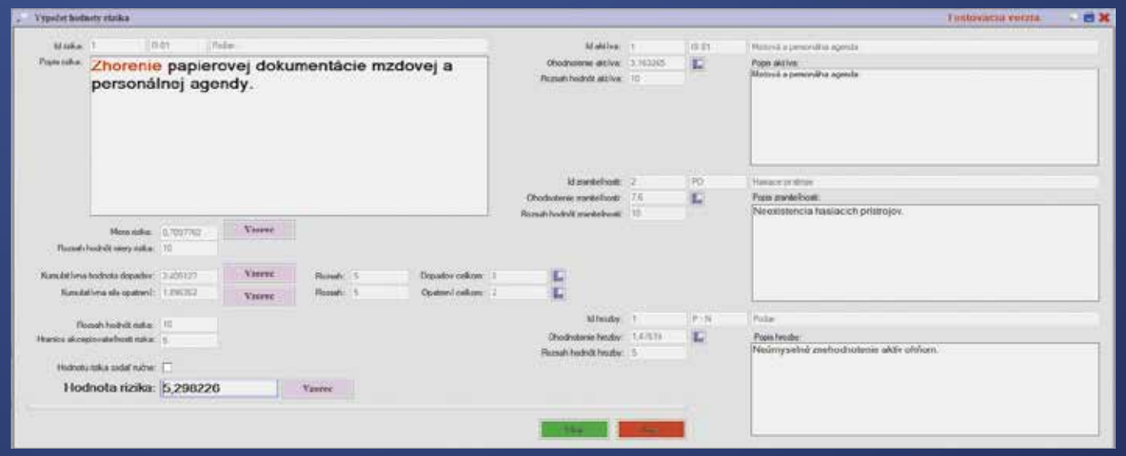
Manažment rizík a v rámci neho analýza rizík je základnou požiadavkou správneho fungovania každého systému riadenia IB.
Keď organizácia chce o sebe prehlásiť, že niečo chráni, mala by jednoznačne vedieť povedať čo chráni, teda musí mať identifikované svoje aktíva (v zmysle IB nie v zmysle účtovníctva). Aktíva musia byť ohodnotené a správne rozkategorizované. K aktívam je potrebné identifikovať ich zraniteľnosti a k zraniteľnostiam priradiť hrozby, ktoré môžu danú zraniteľnosť využiť a realizovať sa na danom aktíve. Táto jedna cesta definuje riziko, ktoré je potrebné ohodnotiť, identifikovať jeho dopady a navrhnúť ochranné opatrenia, ktoré majú riziko eliminovať. Aplikácia ISSR umožňuje v prehľadnej forme všetky hore uvedené prvky evidovať, vrátane vzťahov medzi nimi. Zároveň aplikácia umožňuje každý jeden prvok kategorizovať podľa definovaného druhu, tým je zároveň umožnené zobrazovať zoznamy jednotlivých prvkov v hierarchickej štruktúre (Strom) podľa druhov, alebo v tabuľkovej forme bez štrukturovania.

Manažment riadenia prístupov k aktívam
(Systém evidencie požiadaviek na udelenie a zrušenie prístupu, vedenie záznamov o procese schvaľovania prístupu a o procese jeho realizácie, systém monitoringu a revízie prístupových práv k aktívam.)

Manažment incidentov a komplexná správa databázy incidentov
(Systém zberu informácií o incidentoch IB, vedenie ich zoznamu, riadenie procesu správy incidentov a reakcií na vznikajúce incidenty v zmysle požiadaviek projektu IB.)

V súvislosti s implementáciou Smernice Európskeho parlamentu a Rady 2009/140 ES článku 13a a 13b prebrala Slovenská republika do zákona č. 351/2001 Z. z. o elektronických komunikáciách požiadavky, ktoré sa týkajú integrity a bezpečnosti sietí a služieb spojených s povinnosťou ohlasovania bezpečnostných incidentov vrátane Opatrenia TÚSR č. O-30/2012 z 18.05.2012. V Českej republike je táto problematika definovaná v § 5 písmeno h a § 7 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a ustanoveniach o kybernetické bezpečnostní události a kybernetickém bezpečnostním incidentu. Manažment bezpečnostných incidentov je z hľadiska správneho fungovania systému riadenia informačnej bezpečnosti ďalšou dôležitou časťou systému. Zabezpečuje vlastne akúsi spätnú väzbu, ktorá slúži v procese monitorovania systému riadenia IB na vyhodnocovanie účinnosti prijatých ochranných opatrení, pripadne na návrh nových ochranných opatrení. Aplikácia vedie v prehľadnej forme databázu bezpečnostných incidentov a všetkých činností súvisiacich s riešením daného bezpečnostného incidentu. Okrem toho umožňuje priradiť daný incident ku konkrétnym aktívam, ktorých sa incident týka a tým pádom aj k rizikám, ktoré boli pre dané aktívum identifikované. Z týchto informácií je potom možné vyvodiť závery o účinnosti prijatých bezpečnostných opatrení.

Manažment riadenia kontinuity procesov
(Vedenie zoznamu havarijných plánov a plánov obnovy kontinuity činnosti, ich údržba a aktualizácia v zmysle požiadaviek projektu IB.) Jednou z dôležitých požiadaviek každého systému riadenia IB je mať zdokumentované všetky možné havarijné stavy, ktoré môžu v organizácii nastať. Každý havarijný stav môže ovplyvniť kontinuitu procesov organizácie, preto je potrebné sa dopredu pripraviť na zvládnutie takýchto udalostí. Keď daný havarijný stav nastane je už zvyčajne neskoro tvoriť postupy jeho zvládnutia. Je teda dôležité správne identifikovať a rozkategorizovať havarijné udalosti podľa ich nebezpečnosti na daný proces. Ku každému relevantnému havarijnému stavu je potrebné mať vypracovaný havarijný plán, teda postup, čo robiť v prípade realizácie danej udalosti. Aplikácia ISSR umožňuje v prehľadnej forme evidovať tieto havarijné plány a taktiež informácie o ich revíziách, testovaní prípadne aktivácii.



Všeobecné informácie o ISSR :

Aplikácia ISSR je znalostná aplikácia a zároveň bezpečnostný softvér, ktorý môže obsahovať citlivé údaje prevádzkovateľa. Z tohto dôvodu nie je integrovateľná so všeobecne dostupnými aplikáciami, avšak umožňuje prenos vstupných údajov z iných databáz prevádzkovateľa (napr. pri riadení prístupu alebo štruktúre organizácie). Disponuje viacúrovňovým prístupom. ISSR je softvérový produkt našej spoločnosti, je modifikovateľná pre akúkoľvek spoločnosť, licenčné pokrytie je od jednej plnohodnotnej licencie pre zodpovednú osobu v menších organizáciách, až po licenčné pokrytie pre každú oprávnenú osobu, resp. každého používateľa , s licenčnou politikou pripravenou na mieru konkrétnej organizácie. ISSR je určená výhradne pre koncových používateľov.

ISSR je modulový systém, rozširuje sa podľa potrieb každej organizácie, ktorá zavádza alebo prevádzkuje aj iné systémy riadenia (systém riadenia kvality, environmentu, bezpečnosti a ochrany zdravia pri práci). Softvér ISSR je pod nepretržitým dohľadom autorov aplikácie - manažérov informačnej bezpečnosti, audítorov informačnej bezpečnosti a ochrany osobných údajov, je zabezpečená trvalá kontrola aplikácie a jej súlad s platnou legislatívou a štandardmi. Modulovú aplikáciu ISSR v súčasnosti používajú komerčné aj štátne organizácie, školy, mestá, zdravotnícke zariadenia, tiež Úrad na ochranu OÚ SR, Finančná správa SR, Kancelária NR SR a iné organizácie.

Rozsah 1 licencie ISSR:

Moduly: Ochrana osobných údajov + informačná bezpečnosť + audit + štruktúra organizácie + legislatíva

V štandardnej cene licencie **nie je zahrnuté**: školenie, inštalácia a napĺňanie databáz aplikácie dátami
V štandardnej cene licencie **je zahrnutý**: 1 ročný update odo dňa inštalácie a podpora

Upgrade (aktualizácia) – voliteľná služba:

Po jednom roku je cena upgrade max. 15 % z obstarávacej ceny produktu.

Podporné služby:

- bezplatné poradenské služby na Service DESKu spoločnosti

Platené služby:

Inštalácia, individuálne servisné zásahy, poradenstvo k problematike vrátane bezpečnostnej dokumentácie, služby audítora, naplnenie databáz údajmi z existujúcej dokumentácie spoločnosti.

Doplnkové služby (v oblasti ochrany osobných údajov a IB):

- individuálne školenia pre oprávnené a zodpovedné osoby, pre manažérov IB
- audity stavu riadenia ochrany osobných údajov a informačnej bezpečnosti
- poskytovanie externých služieb Zodpovednej osoby, DPO, poradenské služby
- vypracovanie bezpečnostnej dokumentácie (Projekt na ochranu osobných údajov + smernice + ochranné opatrenia, Projekt informačnej bezpečnosti, doplňujúca dokumentácia)
- spracovanie analýzy rizík
- budovanie účinného systému riadenia informačnej bezpečnosti
- budovanie účinného systému ochrany osobných údajov
- revízie stavu riadenia prostredníctvom kontrolných auditov
- odborná podpora pre zodpovedné osoby, manažérov IB u povinných osôb pred kontrolnými orgánmi

BEZPEČNOSŤ
INFORMAČNÝCH SYSTÉMOV

OCHRANA OSOBNÝCH ÚDAJOV
INFORMAČNÁ BEZPEČNOSŤ

Objednávky, konzultácie:
Datasoft Consulting s.r.o. – vlastník autorských majetkových práv
• implementujeme Nariadenie EP a RADY EÚ č. 2016/679
• poskytujeme služby externej Zodpovednej osoby, DPO, bezpečnosti IS, školenia, máme viac než 1.000 referencií
• na problematiku informačnej bezpečnosti a ochranu OÚ sa špecializujeme od roku 2006

Kontaktné údaje Slovenská republika:
Datasoft Consulting s.r.o.
Baračka 85 Trenčianske Teplice
IČO: 36662739, IČ DPH: SK2022229924
OS TN, odd. Sro, vložka č. 16964/R
support@datasoftconsulting.sk
tel. 00421 911 110 305

Kontaktné údaje Česká republika:
Datasoft Consulting Czech s.r.o.
Platnéřská 90/13 Praha 1 Staré Město
IČO: 03374483, DIČ: CZ03374483
Městský soud v Praze, odd. C, vložka 230514
info@datasoftconsulting.sk
tel. 00420 731 864 655

www.issr.sk