Revizija informacijskih sustava: kome treba i što može, a što ne može otkriti

Centar informacijske sigurnosti, FER

Prof. dr. sc. Mario Spremić, CGEIT

Ekonomski fakultet Zagreb

Osobni podaci

- Ekonomski fakultet - Zagreb, Katedra za informatiku
  - Redoviti profesor u trajnom zvanju
  - Obrazovanje: dipl. inž, PMF - Matematika, Mr.sc. PDS IM, Dr.sc. EFZG
  - Gostujući profesor: FER, FOI, EF Lj, EFSA, Imperial College London
- 1995 - 2001. Ledo d.d., Agrokor d.d. (programer, sistem analitičar, sistem inženjer, voditelj projekata)
- 14 knjiga, preko 150 znanstv. i stručnih članaka
- Član prog. odbora i stalni recenzent radova na 20-ak međunarodnih znanstvenih konferencija i 10-ak znanstvenih časopisa
- Voditelj međunarodnih akreditacijskih postupaka (EPAS akreditacija BDiB studija)
- Voditelj BDiB (Bachelor Degree in Business) studija (www.efzg.hr/bdib), Master in Managerial Informatics studija (oba potpuno na engleskom jeziku) i poslijediplomskog studija Informatički menadžment
- Konzultant i IT revizor (digitalna transformacija poslovanja, cyber rizici, cyber sigurnost - 100+ projekata)
  - Reference >2010: Konzum, Tisak, Podravka, ZSE, SKDD, Banka kovanica, Centar banka, Kreditna banka Zagreb, Partner banka, Samoborska banka, Privredna banka Zagreb, Štedbanka, VABA, Agram osiguranje, Allianz, Croatia osiguranje, Jadransko osiguranje, UNIQA osiguranje, HAC, Hoteli Babin kuk, Ministarstvo prometa, Nova Kreditna banka Maribor, Federalna agencija za bankarstvo BiH, …
- ISACA CC Upravni odbor (CGEIT certifikat)

Teme

- Digitalna ekonomija – prilike i rizici
- Cyber rizici
- Što je revizija informacijskih sustava i zašto je trebamo?
- Studije slučajeva

Trendovi u digitalnoj ekonomiji

- **Digitalna ekonomija** – krovni pojam za označavanje novih modela poslovanja, proizvoda, usluga, tržišta i brzorastućih sektora, osobito onih temeljenih na digitalnoj tehnologiji kao osnovnoj infrastrukturi poslovanja
- **Integracija (prožimanje) tehnologija**
  - Primarne digitalne tehnologije: **mobile, social, cloud, big data, IoT**
  - Sekundarne digitalne tehnologije (3D print, dronovi, robotika, virtualna stvarnost, umjetna inteligencija, nosive tehnologije, …)
  - **Infrastruktura** - everything as a service, disaster as a service, security as a service, …), pametni uređaji, BYOD, NFC, RFID, nosive tehnologije, …
- **Integracija progresivnih koncepcija i poslovnih modela** (start-up, korporativno poduzetništvo, 'disruptive innovation', 'design thinking', 'agile', 'custom', consumer oriented')
- **Novi načini vođenja i upravljanja**

Ericsson – 10 tehnoloških trendova

1. **Video prenošen streamingom.** Najkraće rečeno, budućnost televizije više nije klijent koji gleda redoviti program, nego kupac koji naručuje željene sadržaje i gleda ih kad mu to odgovara.
2. **Sve pametniji domovi** – (IoT), razni kućni senzori (trošenje vode ili struje, sigurnost, javljati gdje su članovi porodice ili kućni ljubimci i upravljati većinom kućnih aktivnosti, od upravljanja grijanjem i rasvjetom do naručivanja hrane od strane inteligentnog frižidera).
3. **Neposrednija komunikacija s prijateljima i suradnicima**
4. **Pametni građani u pametnim gradovima** – inteligentne gradske aplikacije.
5. **Ekonomija razmjene i podjele resursa**.
6. **Digitalni novčanik** – će do kraja desetljeća potpuno zamijeniti gotovinu, kreditne kartice i druge tradicionalne oblike plaćanja (bitne promjena platnog prometa, banaka, itd).
7. **Očuvanje privatnosti**.
8. **Tehnologija koja se nosi, produžuje život** – sve više odjeće i predmeta koje nosimo na sebi (Wearables) postaje inteligentno.
9. **Kućanski roboti**.
10. **Sve povezano sa svime**.

Gartner – 10 tehnoloških trendova

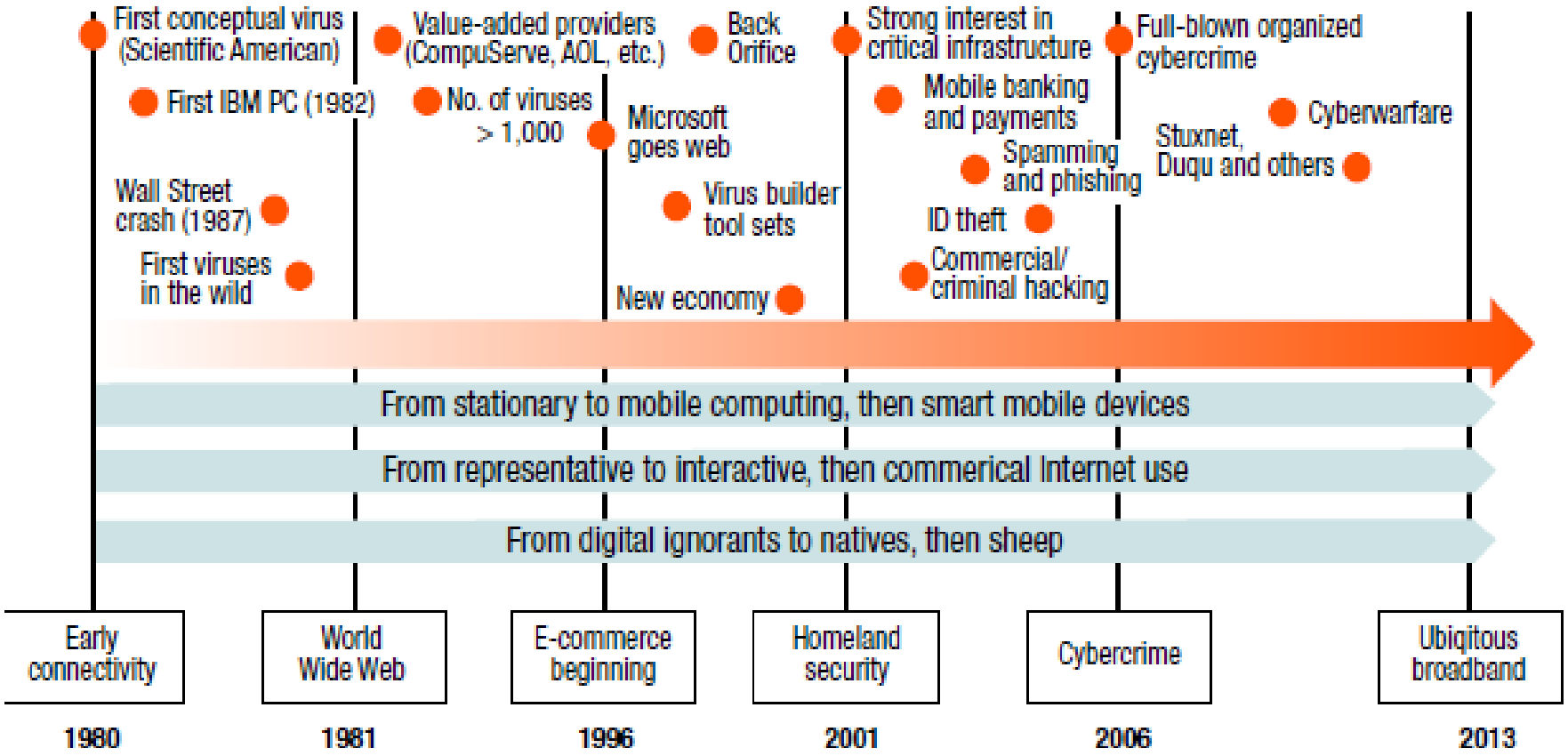
1. **Računarstvo svuda** (Dizajn korisničkog iskustva od presudne važnosti)
2. **Internet of Things (IOT**) (Temelj digitalnog poslovanja)
3. **3D printeri**
4. **Napredne, sveprisutna, nevidljiva analitika**
5. **Kontekstom bogati sustavi**
6. **Pametni strojevi** (autonomna vozila, napredni roboti, virtualni osobni asistenti …)
7. **Cloud / klijent arhitektura**
8. **Sofverski definirana infrastruktura i aplikacije**
9. **Web-Scale IT -** Gartner navodi da će sve više tvrtki morati osmisliti, razvijati i izrađivati aplikacije i infrastrukturu na isti način na koji to rade „giganti“ poput Amazona, Googlea i Facebooka.
10. **Sigurnost i samozaštita sustava temeljeni na riziku**

Informacijski sustavi koji griješe (2000-2010)

NEKI OD POZNATIH SIGURNOSNIH INCIDENATA		
Godina	**Organizacija**	**Opis incidenta**
2007.	TJX Companies	Zbog nezaštićene bežične mreže ukradeni podaci 94 milijuna kreditnih i debitnih kartica.
2007.	HM Revenue & Customs	Izgubljena dva diska s osobnim podacima 25 milijuna obitelji u Velikoj Britaniji.
2007.	HSBC Bank	Kazna od 3,2 milijuna funti zbog gubitka podataka životnog osiguranja od 180.000 klijenata. Uzrok je izgubljeni disk u pošti na kojem podaci nisu bili kriptirani.
2008.	Bank of New York Mellon	Ukradene trake s pričuvnom pohranom podataka iz sistemske sobe. Disk je sadržavao osobne podatke 12,5 milijuna klijenata.
2009.	Heartland Payment System	Izgubljeno oko 130 milijuna podataka o transakcijama zbog infekcije informacijskog sustava zlućudnim kodom.
2011.	Sony Playstation Network	Ukradeno cca. 24 milijuna osobnih podataka, transakcija, zaporki i sl. korisnika Sony Playstation mreže. Gubitak se procjenjuje na 171 milijun dolara.
2001.	Dio Hrvatskog telekoma	Poznati DDoS napadi na hrvatske internetske poslužitelje, što je imalo za posljedicu nemogućnost pristupa Internetu na neko vrijeme.
2002.	Riječka banka	Nestalo je oko 75 milijuna eura putem transakcija koje je godinama vodio diler Riječke banke. Zakazao je kompletan sustav unutarnjih kontrola.

Informacijski sustavi koji griješe (danas)

- Chrysler, Centralne banke Katar i Bangladeš
- Target, Sony, Anthem, Experiean, LOT, Yahoo!
- Stuxnet Iran, prodori u kritičnu nacionalnu infrastrukturu
- USA - cyberprostor je 5. vojna domena - kopno, zrak, more i svemir
- IoE (Incidents of Everyone), BYOD (Bring Your Own Disaster)

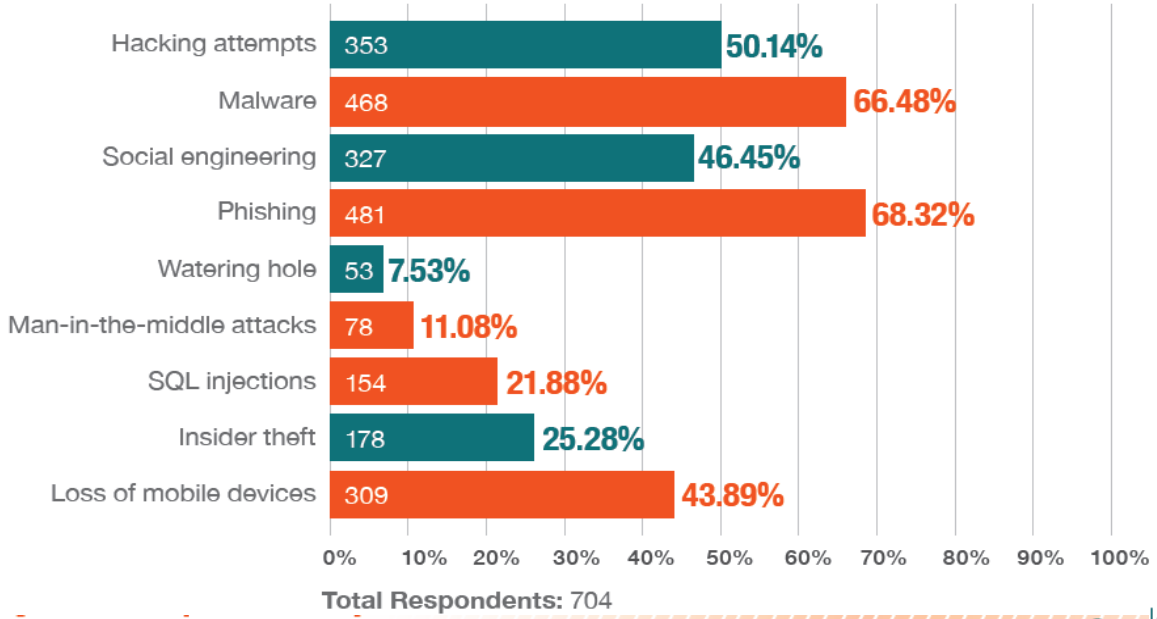


Izazovi i okruženje cyber sigurnosti

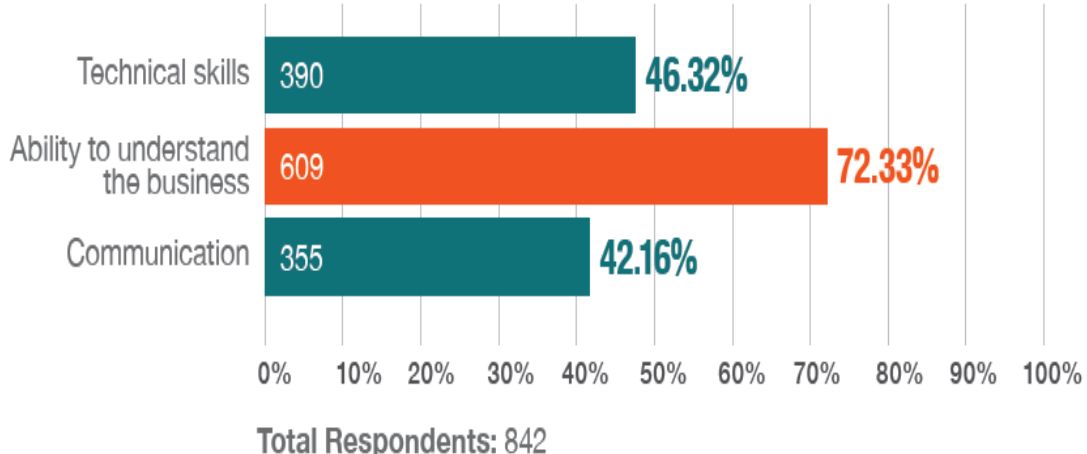
- (McAfee, 2013) trošak cyber kriminala **1000 milijardi USD** (0,2 - 0,4% svjetskog GDP-a, **7% GDP SAD-a**)
- (Washington Post, 2014) trošak zaštitnih mjera od cyber kriminala – **67 milijardi USD** (štete cca 200-njak milijardi USD)
- (ISACA, 2015) **97% cyber napada se moglo izbjeći** da su kompanije imale učinkovite sustave zaštite www.isaca.org/cobit5info-sec
- (ISACA, 2015) **95% kompromitiranih resursa** sadržavalo je povjerljive podatke
- (ISACA, 2015) **šteta od krađa podataka - 174 milijuna USD**, 1 krađa podataka košta 5,5 milijuna USD; razlozi krađe - 58% 'haktivisti', 39% nemar zaposlenih
- (ISACA, 2015) **100 milijardi spam poruka** svaki dan
- (UK Government, 2014) UK cyber crime loss **27 billion GPB**, prevention costs 650 million GPB
- (BBC, 2006) 'most people would disclose their computer password for a chocolate bar'
- Kompanije koje su iskusile sigurnosne informatičke incidente su izgubile prosječno 2,1% svoje vrijednosti uz prosječan gubitak od preko 1,6 milijarda USD po incidentu
- Preko 60% financijskih institucija je doživjelo napad iz područja cyber sigurnosti

Izazovi i okruženje cybersecurity-a (.pdf)

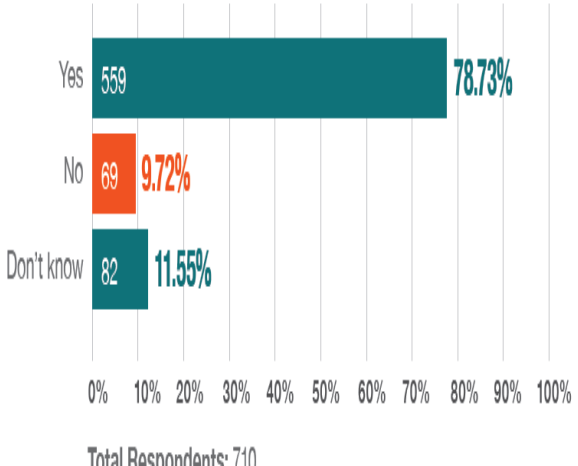
Figure 4—Successful Attack Types
Which of the following attack types have exploited your enterprise in 2014?



What is the biggest skill gap you see in today's security professionals?



Is your board of directors concerned with security?



Sigurnost informacijskih sustava

'Jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, okružen nervnim plinom i dobro plaćenim naoružanim čuvarima. Čak ni tada, ne bih se baš kladio na njega'

Eugene Spafford, director Computer Operations, Audit and Security Technology (COAST)

Ključni aspekti kontrole informacijskih sustava

- **Kontrola je sustav**, što znači da obuhvaća skup uzajamno povezanih (interagirajućih) komponenata koje, djelujući jedinstveno i usklađeno, potpomažu ostvarivanje utvrđenih ciljeva informacijskog sustava.
- Kontrola se usmjerava na **neželjene događaje ili procese** u informacijskom sustavu. Neželjeni događaj može nastati, a proces biti aktiviran zbog neovlaštenih, netočnih, nepotpunih, redundantnih, nedjelotvornih ili neučinkovitih ulaza u sustav.
- Kontrole se primjenjuju zato da bi se **spriječili** (prevenirali), **otkrili** (detektirali) ili **ispravili** (korigirali) neželjeni događaji i/ili procesi.

Kontrole IS-a (informatičke kontrole)

Informatičke kontrole razvrstavamo prema sljedećim kriterijima:

- obzirom na **način primjene** razlikujemo:
  - automatske kontrole,
  - ručne kontrole,
- obzirom **na svrhu** zbog koje se poduzimaju razlikujemo:
  - preventivne kontrole,
  - detektivne kontrole,
  - korektivne kontrole,
- obzirom **na hijerarhijsku razinu** njihova djelovanja razlikujemo:
  - korporativne kontrole,
  - upravljačke kontrole i funkcijske (procesne) kontrole,
  - operativne kontrole,
- obzirom **na način funkcioniranja** razlikujemo:
  - organizacijske,
  - tehnološke i
  - fizičke.

Kontrola vs revizija IS

- Svaki IS, naravno, obiluje brojnim kontrolama koje su u njega ugrađene, a koje se primjenjuju kako bi se ostvarili ciljevi njegova funkcioniranja i kako bi se njime učinkovito upravljalo
- Što su kontrole učinkovitije i dobro oblikovane, manje je vjerojatno da će informacijski sustav biti izložen nekoj prijetnji i da će se neželjeni događaj 'razviti' u rizik za poslovanje
- **Revizijama IS-a** provjeravamo postoji li neka informatička kontrola i kojoj je mjeri učinkovita
- Revizijama IS-a se testiraju razine učinkovitosti informatičkih kontrola, prikupljaju argumenti i dokazi pomoću kojih je moguće procijeniti rizike za poslovanje i dati preporuke za njihovo smanjenje

Revizija IS-a

- **Osnovni ciljevi provedbe revizije informacijskih sustava:**
  - provjeriti trenutno stanje informatike, odnosno utvrditi **razinu zrelosti** upravljanja informacijskim sustavom,
  - provjeriti **(testirati) učinkovitost kontrola** informacijskih sustava, osobito kod ključnih poslovnih procesa,
  - otkriti potencijalno **rizična područja** i procijeniti razinu rizika kojim je poslovanje izloženo temeljem intenzivne primjene informacijskih sustava,
  - dati **preporuke menadžmentu** koje mjere poduzeti da se učinak uočenih rizika smanji ili ukloni i unaprijediti poslovnu praksu po tom pitanju

Regulativa provedbe revizije IS-a

- **Regulativa na međunarodnoj razini (**Sarbanes-Oxley act, Basel II, the European 8th Directive, MiFID)
- **Nacionalna regulativa - kreditne institucije (HNB)**
  - **Odjel za izravni nadzor banaka i fin. Institucija**
  - **Odluka o primjerenom upravljanju IS-om u svrhu smanjenja operativnog rizika**
- **Regulativa specifična za pojedine industrije**
  - **Kartičarske transakcije (PCI DSS)**
  - **Osiguranje (HANFA, Pravilnik o reviziji, članak 12)**
  - **Bankarstvo (Basel III)**
  - **Osiguranje (Solvency II)**
  - **Telekom (eTom)**
  - **Farmaceutska industrija**

Međunarodni certifikati u reviziji IS-a

- **ISACA certifikati (Information System Audit and Control Association)**
  - CISA (Certified Information System Auditor)
  - CISM (Certified Information Security Manager)
  - CGEIT (Certified in Governance of Enterprise IT)
  - CRISC (detalji o svima na www.isaca.org)
- **CISSP (Certified Information System Security Professional)**
- **CIA (Certified Internal Auditor)**
- **Ostali profesionalni i stručni certifikati:**
  - PMP (Project Management Professional)
  - CobiT Foundation
  - ITIL Certificate (www.itil.co.uk)
  - ISO 27001 Lead Auditor
  - Certifikati dobavljača tehnologije (CISCO Academy, Microsoft ‘security’ certifikati, ORACLE ‘security’ certifikati, itd.)

Koraci provedbe revizije IS-a

- Pregled – ‘snimka stanja’ informatike i područja revizije
- Određivanje **područja (objekta)** revizije (ŠTO revidirati?)
  - Određivanje **ciljeva kontrole** za svako područje
- Provedba **testova kontrola** (KAKO revidirati?)
  - Provedba detaljnijih analitičnih testova
- Prikupljanje **dokaza** i procjena poslovnih **rizika** (preporuke)
- Priprema i prezentiranje izvještaja revizora IS-a Upravi

Provedba revizije IS-a

- **Priprema i planiranje (odabir kontrolnih područja i ciljeva, određivanje načina testiranja)**
- Analiza dokumentacije
- Prikupljanje revizijskih dokaza
  - Intervjui, ankete i neformalni razgovori
  - Tehničko ispitivanje i testiranje sustava
- Analiza i vrednovanje revizijskih dokaza
- Analitički testovi (pwd, prava pristupa, pwd1, aix)
- Priprema revizijskog izvješća
- Predstavljanje revizijskog izvješća

Faza revizije informacijskih sustava	% od ukupnog vremena trajanja revizija
Priprema i planiranje	10
Analiza dokumentacije	10
Prikupljanje revizijskih dokaza: – Intervjui, ankete i neformalni razgovori – Tehničko ispitivanje i testiranje sustava	10 15
Analiza i vrednovanje revizijskih dokaza	20
Priprema revizijskog izvješća	20
Predstavljanje revizijskog izvješća	5
Postrevizijske aktivnosti	10

Najčešće korišteni okviri upravljanja cyber rizicima i cyber-sigurnosti

- ISACA Security Publications (**CobiT 5** = 37 kontrolnih područja - KP, Cybersecurity Nexus - **CSX**)
- ISO 27001:2013 (**Annex A**, 14 KP, 35 KC, 133 SKM) (.pdf)
- US National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (5 KP, 25 KC) http://www.nist.gov/cyberframework/ (.pdf)
- **SANS** Institute Critical Controls (4 KP, 20 KC) (http://www.sans.org/critical-security-controls (.pdf)
- **PCI DSS**
- EU uredba **GDPR** (General Data Protection Regulation) – za svako curenje podataka kazna do 4% prihoda ili max 20 mil. EUR

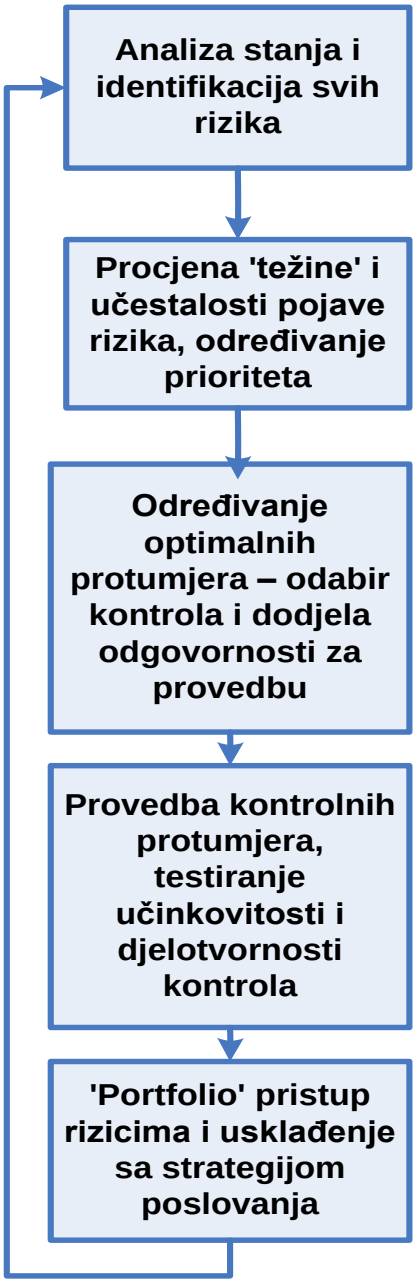
Revizija informacijskih sustava i cyber (IT) rizici

- **Cyber rizici** (informatički rizici, IT rizici) su poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije u okruženju digitalne ekonomije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i poslovanja uopće
- **RIZIK = f (imovina, prijetnja, ranjivost)**
- **Cyber rizici (informatički rizici) imaju dualnu narav:**
  - uvijek su prisutni i
  - dobro vođene informatičke inicijative stvaraju novu vrijednost, nove poslovne prilike i održivu konkurentsku prednost
  - loše vođeni informatičke inicijative uništavaju poslovanje, ne stvaraju novu vrijednost, a troše resurse poslovanja, stvaraju gubitke i frustracije zaposlenika, stvaraju štete i probleme

CIKLUSI CYBER PRIJETNJE (CYBER RIZIKA)

- ‘Izviđanje’, ‘njuškanje’, analiza ranjivosti
- Istraživanja uočene ranjivosti i priprema probnog napada
- Probni cyber napad
- Analiza učinka napada, ‘učenje’ o kontrolama koje ga trebaju otkriti i spriječiti
- ‘Dorada’ cyber napada
- Sljedeći probni napadi
- Veći napadi usmjereni na počinjenje štete

Proces upravljanja IT rizikom



Formalan popis svih informatičkih rizika, pregled prijetnji, ranjivosti (slabosti) sustava, procjena očekivanih negativnih učinaka, klasifikacija rizika prema unaprijed utvrđenim kompanijskim standardima, kategorizacija uzroka i 'okidača' događajima, određivanje vjerojatnosti nastanka i dodjela odgovornosti za svaki rizik ('vlasnik rizika')

Temeljem vjerojatnosti, učestalosti nastanka i procjene ***utjecaja rizika na poslovanje*** (engl. Business impact analysis – BIA) određuju se prioriteti i utvrđuje način upravljanja rizicima
Kvantifikacija težine i frekvencije rizika
Kvalitativno određivanje težine i frekvencije rizika

Određivanje strategije upravljanja rizicima:
- ***prihvaćanje i praćenje razine rizika***
- ***smanjenje 'težine' ili vjerojatnosti nastanka rizika*** - ***određivanje učinkovitih informatičkih kontrola***
- ***izbjegavanje rizika ('prebacivanje' rizika)***
- ***podjela, djelomično 'pokrivanje' rizika***

Izbor najboljih protumjera, dodjela odgovornosti za provedbu (budžet, ciljevi, vremenski rokovi, plan provedbe, vlasništvo nad rizicima)

Da bi se utvrdilo jesu li IT kontrole koje smo implementirali utjecale na smanjenje ključnih rizika i u kojoj mjeri su one djelotvorne i učinkovite, provodi se postupak ***revizije informacijskih sustava*** prema poznatim okvirima (CobiT, ISO 27000, PCI DSS, NIST)
Otklanjanje šteta i procjena **preostalog** (rezidualnog) **rizika** – rizika nakon provedbe kontrolnih protumjera

Povezivanje i usklađenje rizika sa strategijom poslovanja, stalni nadzor i ažuriranje plana upravljanja informatičkim rizicima
Postimplementacijska analiza
Nadzor, revizija i prilagodba plana upravljanja informatičkim rizicima

Prihvatljiva razina rizika - onaj intenzitet rizika koji još uvijek ne ugrožava odvijanje važnih poslovnih funkcija i procesa, odnosno ostvarenje zacrtanih poslovnih ciljeva

UPRAVLJANJE CYBER RIZICIMA

- Analiza svih cyber prijetnji, osobito aktualnih (‘novijih’)
- Istraživanje načina funkcioniranja cyber prijetnje
- Pregled učinkovitosti kontrola koje sprječavaju cyber prijetnje (provjera ranjivosti)
- Ojačavanje kontrola i testiranje njihove učinkovitosti
- Provedba kontrola i revizija (ocjena) njihova rada
- Educiranje korisnika o novim kontrolama i novim prijetnjama

Primjeri cyber napada i mogućih kontrolnih mehanizama

Target – jedan od najvećih maloprodajnih lanaca na svijetu

- 1.800 prodajnih mjesta, 350.000 zaposlenika
- ukupni prihod u 2014. 72 milijarde USD
- 12/2013 – krađa 40 milijuna brojeva kreditnih kartica, preko 70 milijuna adresa, brojeva telefona i ostalih povjerljivih podataka kupaca
- Shvatili da su napadnuti nakon 18 dana, obavijestilo ih ministarstvo pravosuđa

Napad: Fazio Mechanical generic user account s prekomjernim 'rolama'

- Nije bilo segmentacije mreže, niti nadzora prometa, neometan put do POS uređaja
- Malware na POS uređajima
- Prvih nekoliko dana testirali malware, instalacija na sve POS uređaje preko redovite nadogradnje

Šteta: pad profita za 46%, troškovi sanacije oko 300 milijuna USD

- Pad cijene dionice za 15 USD
- Kriminalci prodali podatke oko 3 milijuna korisnika kartica za 18-35 USD

- Da je provedena, što bi revizija IS-a otkrila? Koje kontrole bi spriječile napad?
- Koja kontrolna područja bi trebalo provjeravati?

Primjeri cyber napada i mogućih kontrolnih mehanizama

- **Što je Target uradio?**
- Novi POS uređaji (200 milijuna USD), TargetRed Card (kartice s čipom), CISO

- **Što je otkrila naknadna revizija informacijskog sustava?**
  - jako loše upravljanje lozinkama (uspješno provaljeno 86%)
  - zastarjeli software-i
  - nedovoljno odvojeni sustavi (VLAN)
  - previše osoba s generičkim i/ili prekomjernim pristupom u sustav
  - loša enkripcija podataka na POS terminalima
  - lako dostupni podaci o sigurnosti Targetovog sustava običnim pretraživanjem
  - revizori su uspjeli pristupiti POS terminalu hakiranjem digitalne vage u drugoj prodavaonici

Koje kontrole bi spriječile ovaj cyber napad?

Osnovna revizija informacijskih sustava

- Provjera korisničkih računa (generic users, dormant accounts, outsourcing account, remote users, … UAM)
- Provjera lozinki i ‘rola’ korisnika
- Osnovna revizija mreže (pristup izvana, open ports, OS security settings, sigurnosna konfiguracija ključnih uređaja, pristup uređajima, servisi sigurnog prijenosa sadržaja, …..)
- Zaštita podataka u prijenosu (kriptiranje) i mirovanju (DBMS security settings, zaštita internog povjerljivog prometa)
- Segmentacija mreže
- Antivirusni softver (politike, ažurnost, na koje uređaje se ‘spušta’, itd.)
- Zaštita ključnih uređaja (FW, routeri, POS uređaji)
- Nadzor mrežnog prometa, ‘security triggers’
- Podizanje svijesti zaposlenih o cyber sigurnosti

Primjeri cyber napada i mogućih kontrolnih mehanizama

Centralna banka Bangladeš

- 80 milijuna USD prebačeni na privatne račune u nizu transakcija
- Nova transakcija nije uspjela radi banalne pravopisne pogreške (Deutsche Bank zatražio provjeru naloga od 20 milijuna USD jer je na njemu pisalo ‘fandation’)

Napad

- Ukradene ciljane ‘role’, odobrenja isplate transakcija
- ‘Izviđanje’ što se može učiniti i kakva je zaštita
- Pristup sustavu nezaštićen, previše prekomjernih ‘rola’ i generičkih računa
- SWIFT izlaz potpuno nezaštićen, nema VLANa
- Vrlo jeftini, neprogramabilni routeri (10-ak USD), nikakva zaštita pristupa mreži
- No ‘job log’ (‘second hand’ routeri i slična ostala oprema)

Što bi revizija IS-a otkrila, a što ne?

- Da je provedena, što bi revizija IS-a otkrila? Koje kontrole bi spriječile napad?
- Koja kontrolna područja bi trebalo provjeravati?

Primjeri cyber napada i mogućih kontrolnih mehanizama

Chrysler automobili

- U srpnju 2015. hakeri Chris Valasek i Charlie Müller su daljinskim putem hakirali automobil Jeep Cherokee džip dok se vozio po autocesti (to su napravili doslovno iz kauča, udaljeni 15-ak km)

Šteta

- Opoziv 1,4 milijuna vozila, popravljanje štete, promjena industrijskih i regulatornih pravila

Što bi revizija IS-a otkrila, a što ne?

Primjeri cyber napada i mogućih kontrolnih mehanizama

Sony Entertainment Company

- 24.11.2014. cyber napad, krađa povjerljivih podataka (100 terabajta – pristupni podaci, adrese, 'social security number', brojevi putovnica i viza za holivudske glumačke zvijezde, zdravstvene kartone zaposlenika i brojnih suradnika, povjerljivi podaci o serijama i filmovima koji su se tek trebali početi emitirati

Šteta

- 15 milijuna USD troškovi istraživanja i utvrđivanja činjenica (Sony)
- Troškovi prema partnerima ???
- Reputacijski troškovi

Što bi revizija IS-a otkrila, a što ne?

Što bi revizija IS-a otkrila, a što ne?

ComAir zrakoplovna kompanija

- Do 2004. regionalni lider, 200 letova dnevno, oko 5.000 zaposlenika
- Božić 2004, prekid rada transakcijskog sustava
- BCP i DRP ne postoji, nema plana ‘ručnog’ rada
- Zrakoplovi 5 dana ne mogu poletjeti, rasporeda posada nema

Šteta

- Tisuće putnika provelo božićne blagdane u zračnim lukama
- Izravna financijska šteta 40 milijuna USD, neizravna mnogostruko veća
- Tužbe, inspekcija federalnih tijela, narušen ugled = prodaja kompanije

Što je otkrila naknadna revizija IS-a?

- Kaotično vođenje informatike
- Potpuno nerazumijevanje uloge IT-a u poslovanju od strane Uprave
- Sustav nije otkazao radi prastarih AIX poslužitelja (iz 1986), nego radi logičke pogreške u algoritmima
- Nitko nikada nije napravio internu niti eksternu reviziju IS-a
- Kada su je napravili bilo je prilično kasno

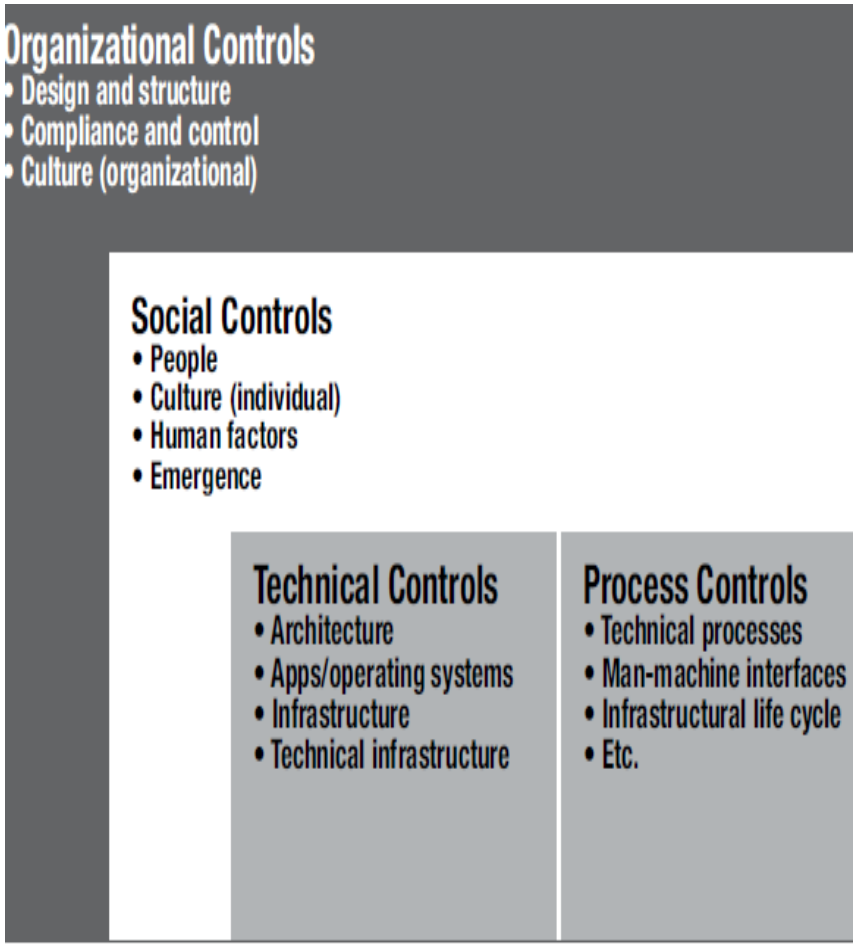
Upravljanje cyber rizicima – R = f (I,P,R)

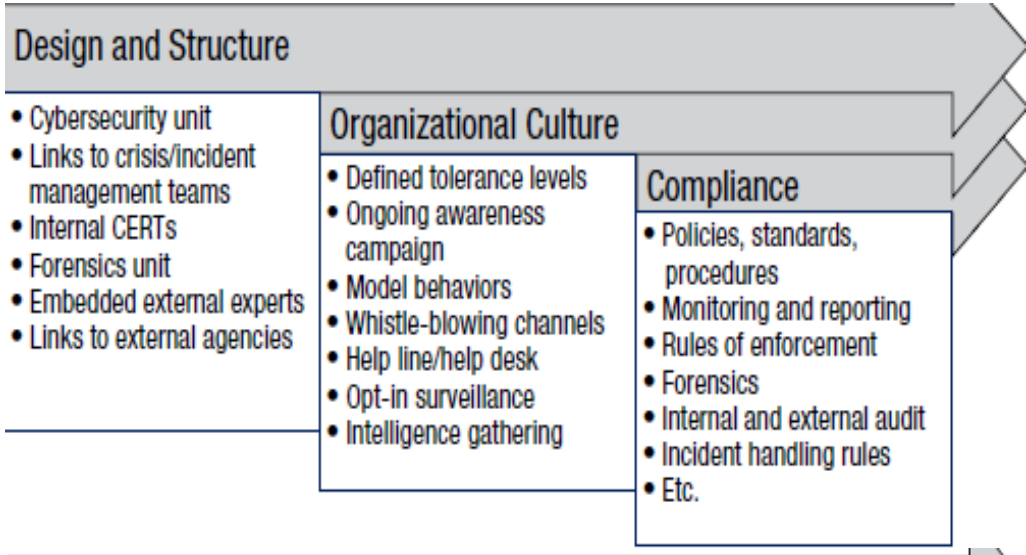
Vulnerability	Threat	Risk and Impact
Spear phishing	Attackers may gain access through phish payload or combined social-technical follow-up.	Initial data loss or leakage leading to secondary financial and operational impact
Water holing	Attackers may gain control of attractive web sites and subsequent control of visitors.	Initial behavioral errors leading to secondary financial and operational impact
Wireless/mobile APT	Attacks may compromise wireless channels and/or mobile devices to enable temporary or permanent control.	Partial or full control of one or more wireless installations and/or mobile devices; direct or indirect impact on all critical IT applications and services
Zero-day	Attacks use zero-day exploits to circumvent existing defenses.	Partial or full control of applications and underlying systems/infrastructure, leading to secondary operational impact
Excessive privilege	Inside attacks may happen using inappropriate privileges and access rights.	Full and (technically) legitimate control outside the boundaries of organizational GRC, secondary financial, operational and reputational impacts
Social engineering	Attackers exploit social vulnerabilities to gain access to information and/or systems.	Partial or full control of human target(s), subsequent compromise of IT side, secondary impacts on personal/individual well-being
Home user APT	Attacks use the fact that home environments may be less well protected than organizational environments.	Partial or full control of applications, systems and home infrastructures, secondary financial, operational and reputational impacts, including impacts on personal/individual well-being
Extended IT infrastructure APT	Attacks may target the IT infrastructure underlying critical organizational processes.	Full control of infrastructure, risk of extended control, including public infrastructures or business partners
Non-IT technical infrastructure APT	Attacks may tunnel the barrier between IT and other critical infrastructures within the enterprise.	Partial or full control of nonstandard IT and technical infrastructure, e.g., supervisory control and data acquisition (SCADA), secondary operational impact
Vendor/business partner exploit	There are attacks on trusted business partners or vendors, compromising key software or deliverables.	Initial attack through organizational IT directed at third parties, with financial, operational and reputational impact

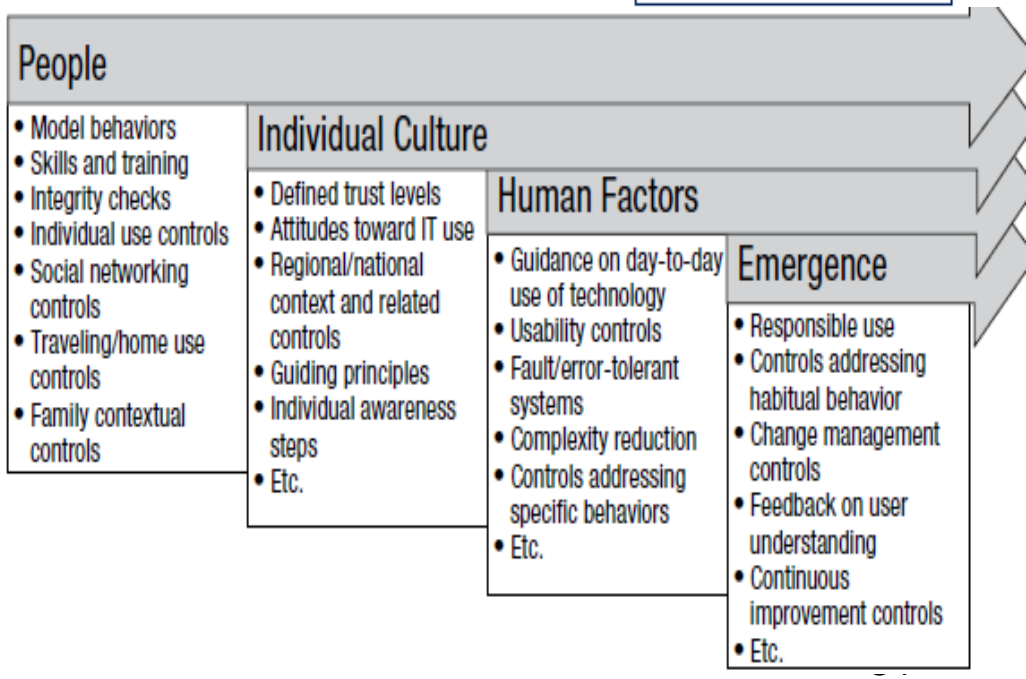
Upravljanje cyber rizicima – R = f (I,P,R) + M,O,E

Vulnerability	Motive	Opportunity	Effort
Spear phishing	Financial, competitive espionage, data theft, etc.; often preparatory to main attack	Email access to target	Medium to high, depending on quality of phish
Water holing	Financial, competitive espionage, data theft, etc.; often preparatory to main attack	Email access to target, control of attractive web sites (the watering holes)	High, depending on precision of targeting
Wireless/mobile APT	Financial, espionage, blackmail/extortion, theft of personally identifiable information (PII), etc.	(Temporary) proximity to target	Low[12] to medium
Zero-day	Financial, operational, data theft, blackmail/extortion, control of technical infrastructure	Availability of suitable zero-day exploits, organized handling of exploits	Medium to high
Excessive privilege	Financial, personal (e.g., disgruntled employee), data theft, blackmail/extortion, reputational	Deficiencies in identity and access management, corruption, etc.	Low to medium
Home user APT	Financial, espionage, data theft, theft of PII, etc.	Physical or logical access to target	Low to high, depending on level of protection of target environment
Extended IT infrastructure APT	Operational, blackmail/ extortion, control of technical infrastructure, data corruption or deletion, cyberwarfare	Logical access to target, often preceded by other forms of attack	High to very high, depending on level of protection of target environment
Non-IT technical infrastructure APT	Operational, blackmail/ extortion, control of technical infrastructure, data corruption or deletion, cyberwarfare	Logical access to target, often preceded by other forms of attack	High to very high, depending on level of protection of target environment
Vendor/business partner exploit	Financial, personal (e.g., disgruntled employee), data theft, blackmail/ extortion, reputational	Logical access to target, often preceded by other forms of attack	Low to high, depending on effort needed for introductory attacks

Upravljanje cyber rizicima – R = f (I,P,R)







Zašto provoditi provjere rada (revizije) IS-a?

- Postoje li i jesu li učinkoviti mehanizmi upravljanja IS-om?
- Jesu li podaci korektno obrađeni i korišteni (prijenos salda-konti – glavna knjiga)?
- Jesu li su u transakcijskim bazama vidljivi učinci provedbe transakcija (promjene nastale izvršavanjem aplikacija – poslovnih procesa)?
- Ima li duplih transakcija (duplih faktura, duplih kupaca i ostalih matičnih podataka)?
- Ima li praznina među evidencijama podataka?
- Prati li klijent neuobičajene transakcije? Može(te) li otkriti zloporabu?
- Kada ste posljednji put provjerili rade li određeni algoritmi pomoću kojih se automatizmom provode poslovne transakcije točno i pouzdano?
- Postoji li mogućnost da netko neovlašten prati/mijenja/unosi podatke i programe?
- Je li moguće da uređajima i ostaloj IT-i može pristupiti netko neovlašten, mijenjati konfiguracije i ugroziti prijenos podataka?
- Je li prijenos podataka među za poslovanje važnim aplikacijama siguran (koriste li se sigurnosni protokoli, može li netko presresti i promijeniti podatke)?
- Kakav je pristup sustavu/aplikaciji?
- Je su li ulazni podaci potvrđeni i ispravni?
- Je li mrežno okruženje sigurno i pouzdano za prijenos podataka? ……

Što bi revizija IS-a otkrila, a što ne?

- Kako se donose odluke o (strateškim i prioritetnim) ulaganjima u informatiku (postoje li odgovarajuće procedure, organizacijska pravila ili preporuke oko toga)?
- Pomoću kojih analitičkih metoda se procjenjuje isplativost ulaganja u informatiku?
- Tko donosi (odobrava) odluke o ulaganjima u informatiku? Tko je odgovoran za provedbu tih odluka?
- Je li naš trenutni poslovni model primjeren trendovima digitalne ekonomije i omogućuje li ostvarenje ciljeva poslovanja?
- Što je zadatak i uloga primjene digitalne tehnologije u poslovanju naše kompanije?
- Imamo li strateški plan primjene digitalne tehnologije? Je li trenutna uloga digitalne tehnologije i informatike prilagođena strateškim ciljevima poslovanja?
- Možemo li učinkovito i konkurentno poslovati bez primjene digitalne tehnologije i modernih informacijskih sustava?
- Možemo li intenzivnom primjenom digitalne tehnologije pozitivno utjecati na ključne pokazatelje poslovanja?
- Koliko često se o informatici raspravlja na sastancima najvišeg menadžmenta kompanije?
- Možemo li opisati proces upravljanja informatikom i digitalnom tehnologijom (tko je za njega odgovoran, tko donosi važne odluke, temeljem kakvih analiza potreba, tko odlučuje o razini ulaganja u informatiku, tko određuje prioritetne informatičke projekte, kako se donose odluke o ulaganju u digitalne tehnologije..)?
- Koji su prioriteti ulaganja u digitalne tehnologije i moderne informacijske sustave?
- Znamo li kako stvoriti novu poslovnu vrijednost (korist) iz primjene informatike i digitalne tehnologije?
- Koliki je povrat ulaganja u informatiku i digitalne tehnologije?
- Znamo li odrediti prioritetne informatičke projekte i možemo li procijeniti njihov doprinos poslovanju?
- Zašto informatički projekti ne uspijevaju?
- Koji su rizici koji proizlaze iz primjene modernih informacijskih sustava temeljenih na digitalnim tehnologijama?

Što bi revizija IS-a otkrila, a što ne?

- Tko vodi brigu o rizicima primjene informacijskih sustava? Imamo li plan upravljanja informatičkim rizicima?
- Što će se dogoditi s poslovanjem naše kompanije ako informacijski sustav neko vrijeme nije u funkciji? Koliko dugo (par minuta, par sati ili par dana) možemo 'izdržati' ako iz bilo kojeg razloga informacijski sustav nije u punoj funkciji ili je u prekidu njegov rad? Koliku štetu (financijsku prije svega) bismo time pretrpjeli? Imamo li preventivne mjere da to takvog scenarija ne dođe?
- Mjerimo li performanse digitalne tehnologije i modernih informacijskih sustava? Znamo li kako ona utječe na pojedine poslovne procese i poslovanje u cjelini?
- Kako je organiziran rad IT sektora / odjela? Što je zadatak i uloga CIO-a? Tko vodi brigu o digitalizaciji poslovanja?
- Jesu li naši korisnici zadovoljni IT uslugom? Kakvo je njihovo iskustvo korištenja našeg poslovnog modela?
- U kojoj mjeri je naš poslovni model ovisan o vanjskim partnerima?
- Koliko brzo možemo tržištu ponuditi nova, funkcionalna i kvalitetna IT rješenja?
- Omogućava li naša postojeća informatička infrastruktura promjene poslovnog modela?
- U kojoj mjeri je naša informatička infrastruktura modularna, fleksibilna, lako, brzo i jeftino nadogradiva, odnosno u kojoj mjeri je 'kruta', 'troma' i slabo upravljiva i brzo promjenjiva?
- Kako mjerimo učinak digitalne i informacijske tehnologije na poslovanje? Imamo li mehanizme kojima analiziramo njihov doprinos poslovanju?
- Provodimo li redovite interne i eksterne revizije informacijskih sustava?

Zaključak – poslovna korist od revizije informacijskih sustava?

- Revizija informacijskih sustava je analitička komponenta korporativnog upravljanja informatikom
- Provodite li strateške ili ‘samo’ operativne (regulatorne, tehničke) revizije informacijskih sustava?
- Zašto koristite IT u poslovanju? Što je poslovna vrijednost IS? Koji su prioriteti ulaganja u IT? Nadzirete li IT? Upravljate li cyber rizicima?
- Kada ste posljednji put revidirali informacijski sustav i zašto?

Hvala na pozornosti

Pitanja, komentari, prijedlozi, sugestije

mspremic@efzg.hr

www.efzg.hr/mspremic