

Kazalo

- 2 Poglavlje 2: IT upravljanje in menedžment
 - 2.1 Praksa upravljanje IT (informacijska tehnologija) za direktorje in upravne odbore
 - 2.1.1 Upravljanje IT
 - 2.1.2 Okvir dela upravljanja IT
 - 2.1.3 IT strateški odbor
 - 2.1.4 Uravnoteženi kazalniki uspeha (Balanced Scorecard – BSC)
 - 2.1.5 Upravljanje informacijske varnosti
 - 2.2 Strateško planiranje (načrtovanje) IT
 - 2.2.1 IT strateški odbor (IT Steering Committee)
 - 2.3 Politika, procesi, procedure in standardi
 - 2.3.1 Politika informacijske varnosti
 - 2.3.2 Politika zasebnosti (privatnost, Privacy)
 - 2.3.3 Politika klasifikacije (razvrstitev) podatkov
 - 2.3.4 Politika klasifikacije sistemov
 - 2.3.5 Politika klasifikacije fizičnega mesta podjetja (Site)
 - 2.3.6 Politika kontrole dostopa (Access)
 - 2.3.7 Politika mobilnih enot
 - 2.3.8 Politika socialnih medijev
 - 2.3.9 Ostale politike
 - 2.3.10 Procesi in procedure
 - 2.3.11 Standardi
 - 2.3.12 Arhitektura podjetij (Enterprise)
 - 2.3.13 Veljavni zakoni, regulativa in standardi
 - 2.4 Menedžment rizikov (Upravljanje groženj)
 - 2.4.1 Program menedžmenta rizikov
 - 2.4.2 Proces menedžmenta rizikov
 - 2.4.3 Tretiranje (Obravnavanje) rizikov
 - 2.5 Praksa IT menedžmenta
 - 2.5.1 Menedžment osebja
 - 2.5.2 Viri
 - 2.5.3 Menedžment sprememb
 - 2.5.4 Menedžment financ
 - 2.5.5 Menedžment kakovosti (kvalitete)
 - 2.5.6 Menedžment portfelja
 - 2.5.7 Menedžment kontrole
 - 2.5.8 Menedžment varnosti
 - 2.5.9 Menedžment sposobnosti (Performance) in zmogljivosti (Capacity)
 - 2.6 Organizacijska struktura in odgovornost
 - 2.6.1 Vloge in odgovornost
 - 2.6.2 Ločitev (segregacija) nalog
 - 2.7 Revizija (Audit) IT upravljanja
 - 2.7.1 Revizija dokumentacije in zapisov
 - 2.7.2 Revizija pogodb z dobavitelji
 - 2.7.3 Revizija zunanjega izvajanja (Outsourcing – ITO)

- 4 Poglavlje 4: Menedžment življenjskega cikla IT
 - 4.1 Realizacija koristi
 - 4.1.1 Menedžment portfelja in programa
 - 4.1.2 Razvoj poslovnih primerov (Business Case)
 - 4.1.3 Merjenje poslovnih koristi
 - 4.2 Projektni menedžment
 - 4.2.1 Organizacija projekta
 - 4.2.2 Razvoj ciljev projekta
 - 4.2.3 Menedžment (Upravljanje) projekta
 - 4.2.4 Projektne vloge in odgovornosti
 - 4.2.5 Plan projekta
 - 4.2.6 Metodologije projektnega menedžmenta
 - 4.3 Življenjski cikel razvoja sistemov (Systems Development Life Cycle – SDLC)
 - 4.3.1 Faze SDLC
 - 4.3.2 Riziki razvoja programske opreme (Software)
 - 4.3.3 Alternativni pristopi in tehnike razvoja programske opreme
 - 4.3.4 Orodja (Tools) razvoja sistemov 35
 - 4.3.5 Pridobivanje infrastrukture in aplikacij baziranih-v-oblaku (Cloud-Based)
 - 4.4 Razvoj in implementacija infrastrukture
 - 4.4.1 Pregled obstoječih tehnologij
 - 4.4.2 Zahteve
 - 4.4.3 Dizajn
 - 4.4.4 Nabava
 - 4.4.5 Testiranje
 - 4.4.6 Implementacija
 - 4.4.7 Vzdrževanje
 - 4.5 Vzdrževanje informacijskih sistemov
 - 4.5.1 Menedžment sprememb
 - 4.5.2 Menedžment konfiguracij

- 4.6 Poslovni procesi
 - 4.6.1 Življenjski cikel poslovnih procesov in re-inženiring procesov
 - 4.6.2 Sposobnostno-zrelostni model (Capability Maturity Model)
- 4.7 Menedžment tretjih-strank
 - 4.7.1 Faktorji rizika
 - 4.7.2 Sodelovanje in skrbni pregled
 - 4.7.3 Klasifikacija
 - 4.7.4 Ocena
 - 4.7.5 Sanacija
 - 4.7.6 Poročilo rizikov
- 4.8 Kontrole podatkov aplikacij
 - 4.8.1 Kontrola vhoda podatkov
 - 4.8.2 Kontrola procesiranja podatkov
 - 4.8.3 Kontrola izhoda podatkov
- 4.9 Revizija življenjskega cikla razvoja sistemov (SDLC)
 - 4.9.1 Revizija programa/projekta in projektnega menedžmenta
 - 4.9.2 Revizija študije izvedljivosti
 - 4.9.3 Revizija potreb oz. zahtev
 - 4.9.4 Revizija dizajna oz. oblikovanja
 - 4.9.5 Revizija nabave aplikacij
 - 4.9.6 Revizija razvoja programske opreme (SW)
 - 4.9.7 Revizija testiranja
 - 4.9.8 Revizija implementacije oz. začetka uporabe
 - 4.9.9 Revizija aktivnosti po-implementaciji
 - 4.9.10 Revizija menedžmenta sprememb
 - 4.9.11 Revizija menedžmenta konfiguracij
- 4.10 Revizija kontrole poslovanja (biznisa)
- 4.11 Revizija kontrole aplikacij
 - 4.11.1 Revizija toka transakcij
 - 4.11.2 Revizija z opazovanjem izvajanja aplikacij na terena
 - 4.11.3 Revizija testa integritete podatkov
 - 4.11.4 Revizija testa interaktivnega (On-Line) procesnega sistema
 - 4.11.5 Revizija procesiranja aplikacij
 - 4.11.6 Revizija kontinuiranega revidiranja
- 4.12 Revizija menedžmenta rizikov tretjih-strank (poslovnih partnerjev)

- 5 Poglavje 5: Menedžment IT servisa in kontinuiteta (neprekinjeno delovanje)
 - 5.1 Delovanje (Operations) informacijskih sistemov
 - 5.1.1 Menedžment in kontrola delovanja
 - 5.1.2 Menedžment IT servisa
 - 5.1.3 Delovanje IT in ravnanje z izjemami
 - 5.1.4 Računalništvo končnih uporabnikov (End-User Computing)
 - 5.1.5 Menedžment knjižnice programske opreme
 - 5.1.6 Zagotavljanje kakovosti
 - 5.1.7 Menedžment varnosti
 - 5.1.8 Kontrola medijev
 - 5.1.9 Menedžment podatkov (Data)
 - 5.2 Strojna oprema informacijskih sistemov
 - 5.2.1 Uporaba računalnika
 - 5.2.2 Arhitektura računalniške strojne opreme
 - 5.2.3 Vzdrževanje strojne opreme
 - 5.2.4 Monitoring strojne opreme
 - 5.3 Arhitekture informacijskih sistemov in programske opreme
 - 5.3.1 Računalniški operacijski sistemi
 - 5.3.2 Programska oprema podatkovnih komunikacij
 - 5.3.3 Datotečni sistemi (File Systems)
 - 5.3.4 Sistemi za upravljanje podatkovnih baz (Database Management Systems – DBMS)
 - 5.3.5 Sistemi za upravljanje medijev
 - 5.3.6 Dodatna (Uporabna) programska oprema (Utility Software)
 - 5.3.7 Licenciranje programske opreme
 - 5.3.8 Menedžment digitalnih pravic
 - 5.4 Infrastruktura mrež
 - 5.4.1 Arhitektura podjetij
 - 5.4.2 Arhitektura mrež
 - 5.4.3 Servisi (Storitve) na osnovi mrež (Network-Based)
 - 5.4.4 Modeli mrež
 - 5.4.5 Mrežne tehnologije
 - 5.5 Stabilnost (Robustnost) poslovanja
 - 5.5.1 Plan kontinuiranega poslovanja (Business Continuity Plan – BCP)
 - 5.5.2 Plan obnove po katastrofi (Disaster Recovery Plan – DRP)
 - 5.6 Revizija IT infrastrukture in delovanja
 - 5.6.1 Revizija strojne opreme (HW) informacijskih sistemov
 - 5.6.2 Revizija operacijskih sistemov (OS)
 - 5.6.3 Revizija datotečnih sistemov
 - 5.6.4 Revizija sistemov za upravljanje podatkovnih baz (DBMS)
 - 5.6.5 Revizija mrežne infrastrukture

- 5.6.6 Revizija kontrole delovanja mrež
- 5.6.7 Revizija IT delovanja
- 5.6.7.1 Revizija delovanja računalnikov (strežnikov, serverjev)
- 5.6.7.2 Revizija menedžmenta datotek
- 5.6.7.3 Revizija vnosa podatkov
- 5.6.8 Revizija delovanja IS brez prisotnosti osebja
- 5.6.9 Revizija menedžmenta problemov delovanja
- 5.6.10 Revizija monitoringa (spremljanja) delovanja
- 5.6.11 Revizija nabave opreme
- 5.6.12 Revizija planiranja kontinuiranega poslovanja (BCP)
- 5.6.12.1 Revizija BC dokumentacije
- 5.6.12.2 Revizija rezultatov predhodnih BC testov in akcijskega plana
- 5.6.12.3 Revizija ključnih oseb
- 5.6.12.4 Revizija pogodb dobaviteljev servisov (storitev)
- 5.6.12.5 Revizija zavarovalnih pogodb
- 5.6.12.6 Revizija arhiva medijev in alternativnega systemskega prostora
- 5.6.13 Revizija planiranja obnove po katastrofi (DRP)
- 5.6.13.1 Revizija plana obnove po katastrofi
- 5.6.13.2 Revizija rezultatov predhodnih DR testov in akcijskega plana
- 5.6.13.3 Revizija arhiva na rezervni lokaciji
- 5.6.13.4 Revizija rezervne (alternativne) procesne opreme

6 Poglavje 6: Zaščita IT sredstev (premoženja, Asset)

- 6.1 Menedžment varnosti informacij
 - 6.1.1 Aspekti menedžmenta varnosti informacij
 - 6.1.2 Vloge in odgovornosti
 - 6.1.3 Uskladitev poslovanja
 - 6.1.4 Popis sredstev in klasifikacija
 - 6.1.5 Kontrola dostopa
 - 6.1.6 Zasebnost
 - 6.1.7 Menedžment tretjih-strank
 - 6.1.8 Varnost človeških virov (Human Resources)
 - 6.1.9 Računalniški kriminal
 - 6.1.10 Menedžment varnostnih incidentov
 - 6.1.11 Forenzično preiskovanje
- 6.2 Logična kontrola dostopa
 - 6.2.1 Koncepti kontrole dostopa
 - 6.2.2 Modeli kontrole dostopa
 - 6.2.3 Grožnje kontrole dostopa
 - 6.2.4 Ranljivost kontrole dostopa
 - 6.2.5 Vstopne točke in metode vstopa
 - 6.2.6 Identifikacija, avtentifikacija in avtorizacija
 - 6.2.7 Zaščita shranjenih informacij
 - 6.2.8 Menedžment uporabniških dostopov
 - 6.2.9 Zaščita mobilnega računalništva
- 6.3 Kontrola varnosti mrež (omrežij)
 - 6.3.1 Varnost mrež
 - 6.3.2 Varnost IoT (Internet of Things)
 - 6.3.3 Varnost aplikacij strežnik-odjemalec (Client-Server)
 - 6.3.4 Varnost brezžičnih (wireless) mrež
 - 6.3.5 Zaščita internetnih komunikacij
 - 6.3.6 Enkripcija (šifriranje, Encryption)
 - 6.3.7 Glas preko IP (Voice over IP - VoIP)
 - 6.3.8 Privatna telefonska stikala (PBX)
 - 6.3.9 Zlonamerna programska oprema (Malware)
 - 6.3.10 Odtokanje (Leakage) informacij
- 6.4 Kontrola okolja
 - 6.4.1 Grožnje in ranljivost zaradi okolja
 - 6.4.2 Kontrola in proti-ukrepi zaradi okolja
- 6.5 Kontrola fizične varnosti
 - 6.5.1 Grožnje in ranljivost zaradi fizičnega dostopa
 - 6.5.2 Kontrola in proti-ukrepi zaradi fizičnega dostopa
- 6.6 Revizija zaščite opreme (sredstev)
 - 6.6.1 Revizija menedžmenta varovanja (varnosti)
 - 6.6.2 Revizija kontrole logičnega dostopa
 - 6.6.2.1 Revizija poti dostopa do mreže
 - 6.6.2.2 Revizija menedžmenta dostopov
 - 6.6.2.2.1 Revizija kontrole uporabniških računov (dostopov)
 - 6.6.2.2.2 Revizija menedžmenta gesel
 - 6.6.2.2.3 Revizija oskrbovanja z uporabniškimi računi (dostopi)
 - 6.6.2.2.4 Revizija ob prenehanju zaposlitve delavca
 - 6.6.2.3 Revizija dnevnikov dostopov (Logs)
 - 6.6.2.4 Revizija preiskovanja in procedure ukrepanja ob incidentih
 - 6.6.2.5 Revizija prisotnosti internetnih točk
 - 6.6.2.5.1 Revizija (Utemeljitev, argumentacija) On-Line (interaktivnih) internetnih dostopov
 - 6.6.3 Revizija kontrole varnosti mrež

- 6.6.3.1 Revizija (Izvajanje pregleda) arhitekture mreže
- 6.6.3.2 Revizija kontrole dostopa do mreže
- 6.6.3.3 Revizija menedžmenta sprememb mreže
- 6.6.3.4 Revizija menedžmenta ranljivosti mreže
- 6.6.4 Revizija kontrole okolja
- 6.6.5 Revizija kontrole fizičnega varovanja
- 6.6.5.1 Revizija položaja in označevanja
- 6.6.5.2 Revizija kontrole fizičnega dostopa