VENDOSJA E TREGUESVE KYÇ TË RISKUT PËR TË FORCUAR MENAXHIMIN E RISKUT TË TEKNOLOGJISË SË INFORMACIONIT DHE PERFORMANCËN E BIZNESIT

***BURAZERI A., VOJ A.**

Alpha Bank Albania, Rr Kavajës, Qendra, Biznesit G-KAM kati 1,Tiranë

e-mail: avoj@alpha.gr

Përmbledhje

Deri më sot, risku i TI dhe çështjet e përputhshmërisë zakonisht nuk marrin nga menaxhimi vëmendjen që meritojnë. Por rritja e incidenteve dhe sofistikimi i risqeve të TI bashkë me ndikimin e tyre në performancën e biznesit, bëjnë të ndjehet nevoja e garantimit të lidhjes së ngushtë midis TKR dhe TKP. TKP të peshuara me risk, ndihmojnë në identifikimin e risqeve që po shfaqen, ul humbjet dhe kostot, minimizon ndërprerjet operacionale, dhe mbron biznesin nga kriza të sigurisë së TI të cilat mund të ndikojnë thellësisht reputacionin. Me ndihmën e një kornize teknologjike robuste, këto TKP dhe TKR mund të përdoren për të shtruar rrugën për një program të suksesshme QKP të TI dhe rritin vlerat për organizatën.

Abstract

As of today, IT risk and compliance issues don't usually get the executive visibility they deserve. But the increasing incidence and sophistication of IT risks and their impact on business performance warrant a tight linkage between KRIs and KPIs. Risk-adjusted KPIs help identify emerging risks, reduce losses and costs, minimize operational disruptions, and protect the business against IT security crises which could deeply impact reputation. With the help of a robust technology framework, these KPIs and KRIs can be used to pave the way for a successful IT-GRC program, and drive increased value for organizations.

Fjalëkyçe: Risku i teknologjisë së informacionit (TI); treguesit kyç të riskut (TKR); treguesit kyç të performancës (TKP); qeverisja, risku dhe përputhshmëria (QRP) e teknologjisë së informacionit (TI).

Hyrje

Në botën e menaxhimit të riskut specialistët përqendrohen në identifikimin e burimit aktual dhe të ardhshëm të riskut dhe, eventualisht, oportunitetet duke përcaktuar dhe monitoruar Treguesit Kyç të Riskut (TKR – eng. Key Risk Indicators - KRI).

TKR janë jashtëzakonisht të dobishëm për departamentin e Teknologjisë së Informacionit (TI)i cili ndeshet me risqe komplekse dhe të rinj që rrjedhin nga përshtatja merisitë informatike: përllogaritja në re (eng. Cloud computing), trendi Sill Pajisjen Tënde (eng. Bring Your Own Device), mobiliteti, virtualizimi dhe menaxhimi i të dhënave të mëdha ndërkohë që kërkohet përputhshmëria me rregullore të shumëfishta, standarde, dhe

korniza siç janë SOX, PCI DSS, HIPAA, FISMA, COBIT dhe ISO 27001. TRK dhe metrikët përkatëse janë kritike për të ndihmuar menaxherët e riskut te TI për të parashikuar risqet në zhvillim si edhe që të jenë të mirëpërgatitur për ti mitiguar ato kur shfaqen.

Rëndësia e TKR

Sipas ISACA [2], TKR janë "metrika të afta të tregojnë që organizata është subjekt ose ka probabilitet të lartë të jetë subjekt i një risku që tejkalon limitet e oreksit të riskut të paracaktuar". TKR lajmërojnë nevojën që të ndërmerren veprime të menjëhershme.

Le të konsiderojmë riskun reputacional – një variabël kompleksi cili prek direkt performancën e biznesit. Risku ndikohet nga shumë faktorë siç janë risitë e produktit, vendi i punës, qeverisja, qytetarët dhe udhëheqja. Por nëse kompania nuk di se cili nga këta faktorë e shkakton riskun atëherë nuk do të jetë në gjendje të përgjigjet me veprimin e duhur.

TKR ndihmojnë që të kuptohet burimi i riskut dhe ngjarjeve qe mund të shkaktojnë probleme të brendshme në organizatë. Ata gjithashtu tregojnë faktorët e mundshëm të jashtëm që mund të ndikojnë në kërkesën dhe ofertën e produkteve dhe/ose shërbimeve të organizatës. TKR mund të jenë raporte të thjeshta që bëhen nga grupet analizuese, ose metrika më të përpunuara që kërkojnë renditje shumë përmasore dhe analiza përpara se të ndërmerren veprime.

Disa nga risqet e mundshme që KRI adresojnë janë:

- Risqet e përputhshmërisë rregullatorë
- Risqet e mashtrimit ose korrupsionit
- Risqet reputacionale
- Risqet e veprimeve të konkurrentëve
- Risqet gjeopolitike
- Risqet raportuese
- Risqet e dinamikës të tregut
- Risqet e sigurisë
- Risqet e ndërprerjes së biznesit
- Risqet e lidhura me talentin
- Risqet kontraktuare

Materiali dhe metodat

TKR përkundrejt Treguesve Kyç të Performancës

COSO [3] i përcakton TKR si "metrika të përdorura nga organizata për të siguruar një sinjalizim të hershëm të rritjes së ekspozimeve me risk në zona të ndryshme të ndërmarrjes". Nga ana tjetër COSO përshkruan Treguesit Kyç të Performancës (TKP – eng. Key Performance Indicators - KPI) si të "skicuar për të siguruar një këndvështrim nga lart të performancës së organizatës dhe të njësive kryesore operacionale të saj. Këto raporte shpesh

janë të përqendruara pothuajse ekskluzivisht në performancën historike të organizatës dhe në njësitë apo operacionet kyçe të saj".

Për nga natyra e tyre, TKP janë esencialisht të "prapambetura" ndërsa TKR janë të "përparuara". Grafiku i mëposhtëm jep më së miri karakteristikat përkatëse

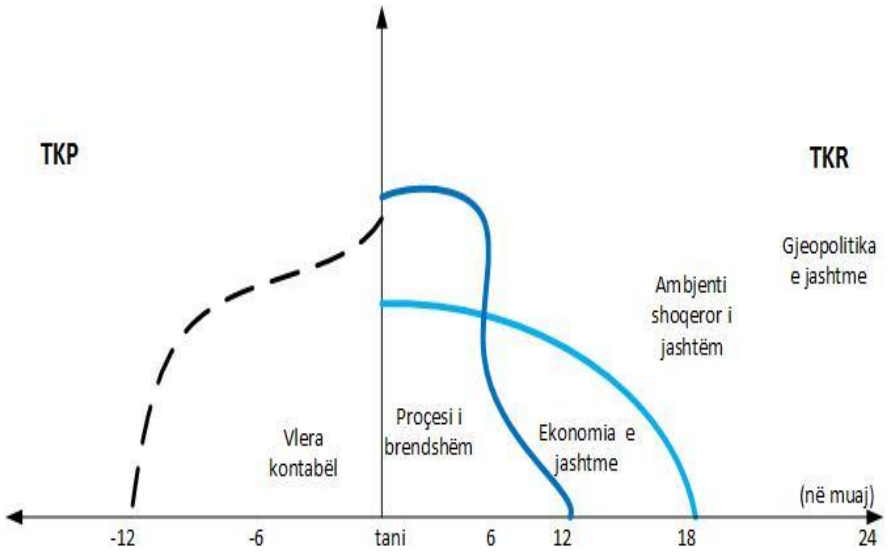


Figura 1. TKP kundrejt TKR

TKP janë qenësisht të rëndësishme për një menaxhim të suksesshëm të çdo organizate, pasi ndihmojnë të identifikohen zonat me nën-performancë të një ndërmarrjeje ashtu si edhe ato aspekte të biznesit që mund të kërkojnë burime apo energji shtesë. Një raport tipik TKP do të përmbante raporte periodike të tendencave të shitjeve, vonesat në arkëtime, dërgesat dhe të dhëna të tjera relevante për organizatën.

Mirëpo, TKP mund të mos sigurojnë tregues të hershëm sinjalet të zhvillimit të risqeve sepse ata kryesisht përqendrohen në rezultatet që tashmë kanë ndodhur. Pikërisht këtu TKR bëhen kritikë të suksesit të cilitdo programi menaxhimi. Aftësia e tyre për të ndihmuar në parashikimin e ngjarjeve të mundshme negative është veçanërisht e dobishme në identifikimin e zonave ku kontrolle shtesë ose planet mitiguese mund të implementohen, apo ku oportunitetet e tregut mund të eksplorohen.

Përzgjedhja e TKR të duhura për sigurinë e informacionit dhe menaxhimit e riskut të TI

Risqet e TI janë një burim domethënës i riskut strategjik dhe kështu është kritike identifikimi i TKR korresponduese. Ndërkohë nuk ka një set standard të TKR që mund të aplikohet përgjatë organizatës, është e nevojshme të niset me krahasimin (eng. benchmarking) të TKR të organizatës me një tjetër. Në

qoftë se dy organizata janë në të njëjtin biznes mundësitë janë që TKR të jenë të përbashkëta.

Në vend të përpjekjes për matjen e të gjitha risqeve të TI, është e rëndësishme të identifikohen ato risqe që kanë ndikim në arritjet afat-shkurtra dhe afat-gjata të objektivave të performancës të organizatës. TKR të TI, duhet të udhëheqin drejt një njohjeje më të thellë se si risqet e TI ndikojnë në performancën e biznesit.

Për të identifikuar TKR e duhura, risqet e njohura duhet të lidhen me nismat kryesore strategjike. Kjo bën që menaxhimi të nisë identifikimin e metrikave më kritike që mund të shërbejnë si TKR udhëheqëse për ti ndihmuar ata në mbikëqyrjen në ekzekutimin e nismave kryesore strategjike. Ky përdorim strategjik i TKR rrit mundësitë që objektivat e vendosura nga menaxhimi të arrihen. Monitorimi pro aktiv TK Relevantë ndihmon në minimizimin e pasigurive dhe identifikimin e mundësive për përshtatjet operacionale ose strategjike.

Disa faktorë për tu marrë parasysh kur zgjidhet bashkësia e përshtatshëm e TKR janë:

- Relevanca - Relevanca ndryshon nga një njësi biznesi tek tjetra. Kështu që TKR duhet të përmbajë nevojat individuale të njësisë së biznesit.
- Matshmëria - TKR duhet të jenë lehtësisht të matshme. Punonjësit nuk duhet të harxhojnë shumë kohë duke mbledhur të dhënat nga burime të ndryshme për ti llogaritur ato.
- Parashikueshmëria - TKR duhet të kenë natyrë parashikuese dhe duhet të vendosen në kontekstin e biznesit për përcaktuar rezultatet e pritshme.

Disa shembuj për TKR për TI janë:

- Operacionet e TI
  - Norma e kthimit të personelit kyç të TI
  - Implementimi i ndryshimeve urgjente
  - Numri i punonjësve me të drejta administrative
  - Numri i makinave me programe të paautorizuara
  - Numri i makinave me përjashtime kundrejt politikave te konfigurimit
- Siguria e Informacionit
  - Numri i vulnerabiliteteve të hapura të larta dhe kritike për server/aplikacion
  - Numri i vulnerabiliteteve të hapura me mundësi shfrytëzimi
  - Mesatarja e ditores së ekspozimit
  - Norma e vulnerabiliteteve të rihapura
  - Vulnerabilitete të larta dhe kritike pa paketa korrigjuese nga shitësi
  - Numri i hyrjeve nga vendndodhje të panjohura

- Përqindja e sistemeve/ aplikimeve/ kontrolleve/ funksioneve të pa testuar të biznesit në 18 muajt e fundit

➢ Audit
- Indeksi i përjashtimeve të auditit = përjashtimet e lejuara përkundrejt totalit të gjetjeve të auditorëve
- Tendenca / norma e rritjes së gjetjeve të auditorëve
- Koha mesatare për zgjidhjen e gjetjeve të auditor
- Numri i gjetjeve kritike / me jo-përputhshmëri rregullatorët të papërmbushura për tremujor

➢ Vazhdimësia e biznesit
- Kostoja mesatare e incidentit
- Incidente për vit
- Përqindja e funksioneve kritike të biznesit pa plan rikuperimit në rast katastrofe
- Përqindja e proceseve ku vazhdimësia e biznesit ose planet rikuperimit në rast katastrofe nuk janë përditësuar / testuar në mbi 12 muaj

Ndërkohë që përcakton TKR, menaxhimi duhet të:

- Konsiderojë riskun në mënyrë eksplicite.

- Punojë drejt TKP të peshuara me riskun për të përmirësuar vendimet e biznesit dhe rritur vlerën e biznesit.

- Zhvillojë një model vlerash të ndërgjegjshme/peshuara me riskun i cili paraqet ngjarjet dhe aktivitetet që ndikojnë rezultatet e pritura ose të planifikuara të organizatës.

Si të sistemojmë TKR për të përmirësuar performancën e biznesit

Për të qenë më efektive TKR duhet të vendosen në kontekstin e biznesit dhe të shoqërohen me TKP korresponduese. Le të marrim riskun e privatësisë së të dhënave. Edhe pse është në një risk i lidhur me TI, ka ndikim në TKP e kënaqësisë të klientit dhe reputacionin e kompanisë. Nga ana tjetër risku i disponibilitetit së sistemit ka ndikim në TKP e ekselencës operacionale. Është e rëndësishme të lidhen TKR e privatësisë së të dhënave dhe disponibilitetit së sistemit me TKP korresponduese.

Çelësi është të fillohet me TKR të besueshme dhe diskrete që ndikojnë direkt mbi TKP e biznesit dhe përkatësisht të ndërtohen "TKP të peshuara me risk".

Një shikim më të thelluar në TKP të peshuara me risk është veçanërisht i rëndësishëm për drejtuesit e larte. Ai i ndihmon ata të kuptojnë se si risku ndikon performancën e biznesit e cila, nga ana e saj, i lejon të marrin vendime strategjike më të informuara dhe efektive me rezultat në rritje për vlerat e biznesit.

TKR, TKP dhe strategjitë mund të lidhen në shumë mënyra. Kjo mund të bëhet, për shembull, duke përdorur "analizën vertikale-horizontale" ku fillimisht çdo palë e interesuar (p.sh. Drejtori Ekzekutiv, Drejtori i Teknologjisë Informacionit, Drejtori i Financës) përcakton cili aktivitet në funksionin e tij është kritike për të arritur objektivat e kompanisë. Pastaj, ata mund të krijojnë lidhjet e vartësisë duke përcaktuar cili aktivitet varet në ngjarjet që ndodhin në zinxhirin e vlerave. Rezultatet sigurojnë një analizë të shkëlqyer të lidhjeve shkakësore për TKP dhe TKR.

Roli i teknologjisë në përcaktimin dhe menaxhimin e TKR

Organizimi, monitorimi, rishikimi, dhe komunikimi i progresit të TKR dhe ndikimi i tyre në TKP mund të lehtësohet dukshëm nga ekzistenca e një kornize teknologjike të përqendruar dhe të automatizuar e cila do të vepronte si një pikë e vetme reference duke i mundësuar organizatës agregimin efikas të informacionit mbi riskun e TI nga burime të shumëfishta, duke përfshirë këtu sistemet e sigurisë së informacionit (p.sh. kërcënimet dhe vulnerabilit etët e aplikimeve) sistemet e përputhshmërisë së TI (p.sh. HIPAA, NERC, ISO) dhe sistemet operacionale të TI (p.sh. performanca, disponibiliteti).

Një kornizë e përqendruar thjeshtëson dhe fut në rrjedhë hartëzimin e risqeve ndaj objektivave dhe kontrolleve të biznesit, të cilat aftësojnë organizatën të menaxhojnë më efektivisht përputhshmërinë me PCI, HIPPA, certifikatat e ISO [1], ligjet e privatësisë, dhe standardet dhe rregulloret e tjera të TI. Gjithashtu mundëson një qasje të integruar për përcaktimin dhe lidhjen e TKP dhe TKR përmes proceseve të ndryshme kryesorë në ndërmarrje dhe duke përcaktuar efektivisht një gjuhë të përbashkët për riskun dhe vizionin.

Mjetet e avancuara teknike mundësojnë vendosjen e kufijve të riskut me anë të sinjalizimeve automatike duke njoftuar kështu personelin e duhur sa herë që një prag shkelet. Si pasojë, organizatat kursejnë kohë, kosto dhe përpjekjet manuale të ndjekjes së TKR dhe pragjeve të riskut.

Aftësitë gjithëpërfshirëse raportuese dhe të ashtuquajturat "kroskote" (eng. Dashboards) ndihmojnë në mbledhjen e të dhënave të riskut përgjatë organizatës dhe ofrojnë një pamje kuptimplotë të TKP të peshuara me riskun. Kjo inteligjencë e riskut është kritike për drejtuesit e lartë për të krahasuar risqet midis bizneseve dhe të përcaktojnë ndikimin e tyre në performancën dhe objektivat strategjike.

Për një efektivitet optimal, teknologjia e përdorur nga organizatat për të menaxhuar riskun e TI dhe TKR duhet të sistemohet për të menaxhuar proceset e përputhshmërisë së TI, auditit të TI, dhe çështjeve të tjera të proceseve kryesore të Qeverisjes, Riskut, dhe Përputhshmërisë (QRP – eng. Governance, Risk, Compliance – GRC) së TI. Akoma më e rëndësishme është vendosja në një linjë e proceseve kryesore të QRP të TI me ato së ndërmarrjes për të lehtësuar një përafrim tërësor dhe të qëndrueshëm ndaj QRP që është ngushtësisht në linjë me strategjinë e biznesit.

Rezultatet dhe diskutime

Implementimi në bankë i TKR dhe TKP – Përllogaritja e aftësisë të rrjetit të degëve të bankës për të ofruar shërbimet bazë bankare.

Përkufizim. Disponibilitet i rrjetit të degëve përkufizohet si aftësia për ti ofruar klientëve shërbime bankare nëpërmjet përdorimit të sistemit bazë bankar (eng. Core Banking system).

Disponibiliteti i rrjetit të degëve matet përgjatë orëve të shërbimit nga 8 deri në 17. Për thjeshtësi përllogaritja e disponibilitetit konsideron se të gjitha degët kanë peshë të njëjtë pavarësisht nga vëllimi i tyre i biznesit apo numri i klientëve/llogarive. Metoda e përshkruar më poshtë mund të aplikohet lehtësisht më tej duke aplikuar teknikat e peshimit të degëve. Përsëri, për thjeshtësi, është marrë e mirëqenë mungesa e mundësive të tjera të dështimit të mundësisë për shërbim siç janë energjia elektrike apo alternativat e saj (kjo për faktin se ne kemi mundësuar furnizim pa ndërprerjeje me energji në degët tona nëpërmjet kombinimit të rrjetit elektrik me gjeneratorë dhe sistem UPS) ose ndonjë ngjarje tjetër negative.

Analiza e disponibilitetit dhe faktorët përbërës:

- Sistemi bazë bankar dhe infrastruktura e tij
Sistemit bazë bankar ngrihet mbi një server aplikimi dhe një server baze të dhënash. Dështimi i cilitdo prej tyre në shërbim çon në dështimin e dsponibilitetit të sistemit prandaj ky komponent matet si mesatarja e kohës disponibël të secilit server.
- Linjat e komunikimit
    - Linja ndërkombëtare e komunikimit ndërmjet serverave të sistemit bazë bankar dhe drejtorisë së përgjithshme të bankës konsiston në një sistem automatik kalimi nga linja primare në rast dështimi tek linja sekondare pa shkaktuar ndërprerje të disponibilitetit të komunikimit. Disponibiliteti i këtij sistemi matet si maksimumi i kohës disponibël së linjës primare dhe asaj sekondare.
    - Komunikimi i degëve me drejtorinë e përgjithshme kryhet me anë të topologjisë "yll" (çdo degë komunikon drejtpërdrejt me drejtorinë nëpërmjet një linje të dedikuar dha anasjelltas). Secila prej këtyre komunikimeve konsiston në një çift linjash (primare dhe sekondare) duke siguruar përsëri kalim automatik nga linja primare tek ajo sekondare në rast dështimi. Përsëri, disponibiliteti i komunikimeve lokale matet si maksimumi i kohës disponibël së linjës primare dhe asaj sekondare.

Disponibiliteti përfundimtar i një dege banke të caktuar matet duke agreguar komponentët e mësipërme. Simbolikisht:

$$D = \frac{(1 - (KM \times (1 - SBB) + KM(1 - LN) + KM(1 - LL))}{KM} \times 100$$

Ku:

D *Disponibiliteti i agreguar i degës i shprehur në përqindje*

SBB *Disponibiliteti i sistemit bazë bankar i shprehur në përqindje*

LN *Disponibiliteti i komunikimit ndërkombëtar i shprehur në përqindje*

LL *Disponibiliteti i komunikimit ndërkombëtar i shprehur në përqindje*

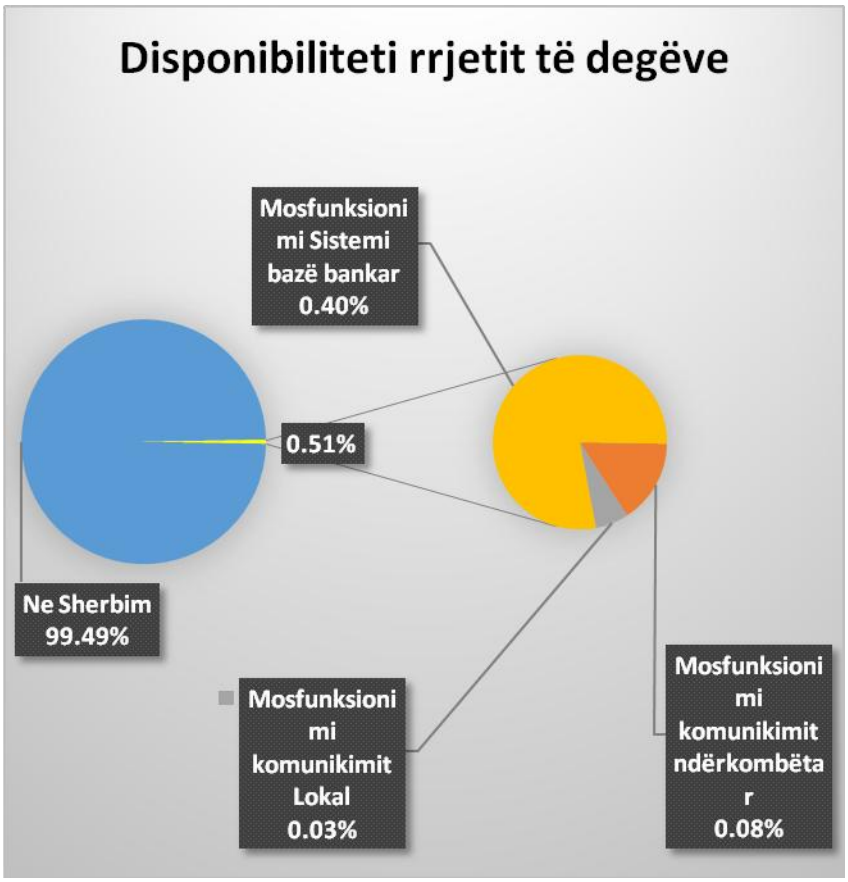
KMM *Koha e monitorimit e shprehur në minuta (540 = 9 orë x 60 minuta)*

Disponibilitet i rrjetit të degëve apo aftësia për ti ofruar klientëve shërbime bankare nëpërmjet përdorimit të sistemit bazë bankar matet si mesatare e thjeshtë e disponibilitetit të gjitha degëve së bashku.

Ilustrime tabelorë dhe grafike.

Dega	Linja ndërkombëtarëparësore	Linja ndërkombëtaredytësore	Disponibiliteti i komunikimit ndërkombëtar	Linja lokale parësorë	Linja lokale dytësorë	Disponibiliteti i komunikimit lokal	Sistemi bazë bankar	Disponibilitet i rrjetit të degëve
Dega 1	99.92	99.87	99.92	99.53	99.93	99.93	99.60	99.45
Dega 2	99.92	99.87	99.92	99.98	99.99	99.99	99.60	99.51
Dega 3	99.92	99.87	99.92	99.96	99.99	99.99	99.60	99.51
Dega 4	99.92	99.87	99.92	99.94	99.98	99.98	99.60	99.50
Dega 5	99.92	99.87	99.92	99.77	99.90	99.90	99.60	99.42
Dega 6	99.92	99.87	99.92	99.99	99.99	99.99	99.60	99.51

Dega 7	99.92	99.87	99.92	100.00	100.00	100.00	99.60	99.52
Dega 8	99.92	99.87	99.92	99.86	99.97	99.97	99.60	99.49
Dega 9	99.92	99.87	99.92	99.97	99.98	99.98	99.60	99.50
Dega 10	99.92	99.87	99.92	99.87	99.94	99.95	99.60	99.47
Banka	99.92	99.87	99.92	99.89	99.97	99.97	99.60	99.49



Përfundime

Deri me sot, risku i TI dhe çështjet e përputhshmërisë zakonisht nuk marrin nga menaxhimi vëmendjen që meritojnë. Por rritja e incidenteve dhe sofistikimi i risqeve të TI bashkë me ndikimin e tyre në performancën e biznesit bëjnë të ndjehet nevoja e garantimit të lidhjes së ngushtë midis TKR dhe TKP. TKP të peshuara me risk ndihmojnë në identifikimin e risqeve që

po shfaqen, ul humbjet dhe kostot, minimizon ndërprerjet operacionale, dhe mbron biznesin nga kriza të sigurisë së TI të cilat mund të ndikojnë thellësisht reputacionin. Me ndihmën e një kornize teknologjike robuste, këto TKP dhe TKR mund të përdoren për të shtruar rrugën për një program të suksesshme QKP të TI dhe rritin vlerat për organizatën.

Literatura

ISO/IEC 27004: 2009

http://www.isaca.org/cobit

http://www.coso.org/documents/COSOKRIPaperFull-FINALforWebPostingDec110_000.pdf