Bazat e Auditimit të IT-së

tirana
EUROPEAN
YOUTH
CAPITAL'22

NATIONAL YOUTH CONGRESS
nyc
Albania
KONGRESI RINOR KOMBËTAR

KONGRESI
RINOR
KOMBËTAR

BASHKIA
TIRANË

Objektivat

- Kuptoni përkufizimin e auditimit të IT-së dhe ciklin e jetës së auditimit
- Mësoni qëllimin e auditimeve të IT-së dhe pse ato kryhen
- Mësoni rreth rreziqeve që rrjedhin nga IT dhe marrëdhëniet e tyre me informacionin financiar
- Mësoni mbi risqet e kontrolleve të IT.

Tabela e Përmbatjes

1. Prezantimi i auditimit të IT-së

Auditimi i IT-së

Përkufizimi i Auditimit të Teknologjisë së Informacionit

Procesi i mbledhjes dhe vlerësimit të evidencave për të përcaktuar nëse sistemet e informacionit dhe burimet përkatëse:

- **mbrojnë në mënyrë të duhur asetet**;
- ruajne **integritetin** dhe **disponueshmërinë** e te dhenave dhe sistemeve;
- ofrojnë informacion të **përshtatshëm** dhe të **besueshëm**;
- për të arritur qëllimet e organizatës në mënyrë **efektive**,
- konsumojnë burimet në mënyrë **efikase**
- kanë kontrolle të brendshme që ofrojnë siguri të arsyeshme se objektivat e biznesit do të përmbushen dhe ngjarjet e padëshiruara do të parandalohen, ose zbulohen dhe korrigjohen në kohën e duhur.

ISACA

Lloje të tjera të auditimeve të TI-së

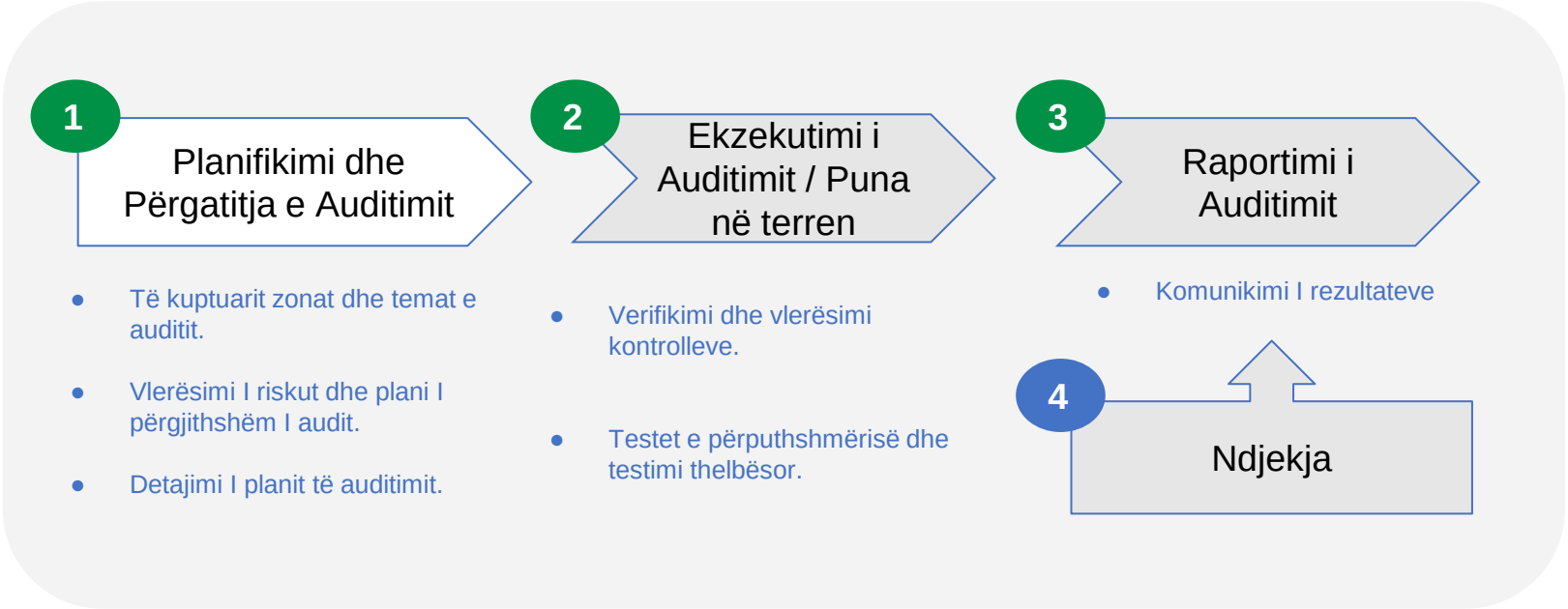
Auditi Financiar

Auditimi financiar kërkon të vlerësojë korrektësinë e pasqyrave financiare të një organizate. Auditimi i IT-së vjen në auditimin financiar për të vlerësuar nëse sistemet e informacionit dhe burimet përkatëse (përfshirë informacionin) mbrojnë në mënyrë adekuate integritetin e të dhënave.

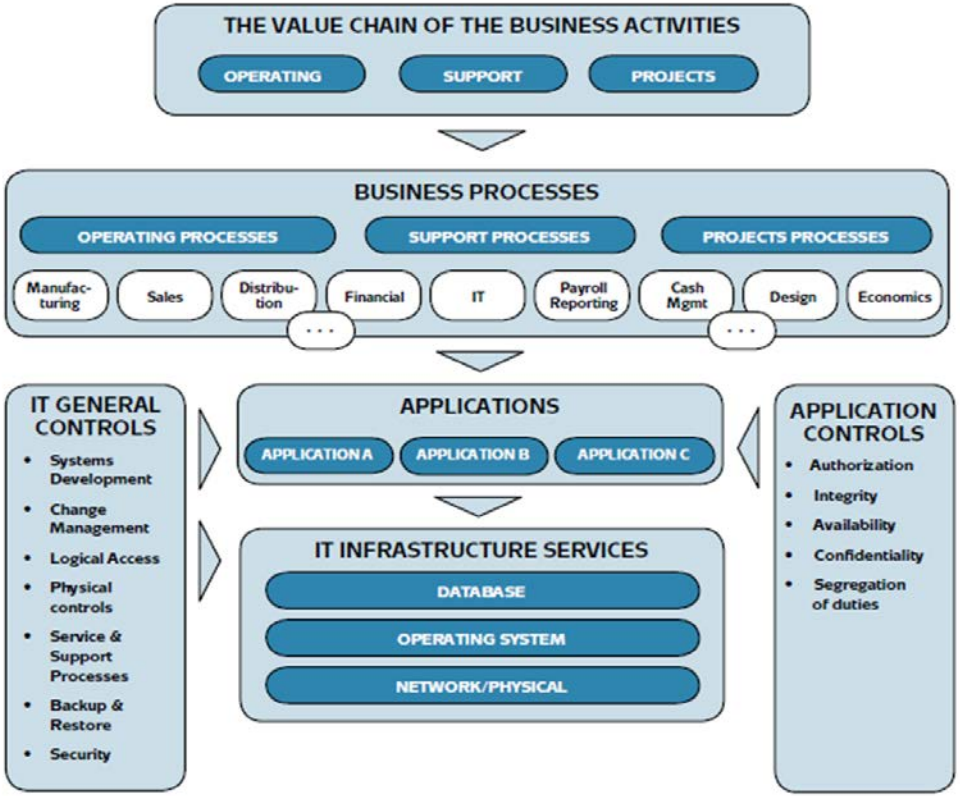
Auditimet e përputhshmërisë

Auditimi i përputhshmërisë përfshin teste specifike të kontrolleve për të kontrolluar respektimin e rregulloreve dhe standardeve specifike. Këto auditime shpesh mbivendosen me auditimet tradicionale të TI-së, por mund të fokusohen në sisteme ose të dhëna të veçanta.

Cikli jetësor i auditimit të IT



Mjedisi i biznesit dhe IT



Një **proçes biznesi** është një koleksion aktivitetesh ose detyrash të lidhura, të strukturuara nga njerëzit ose pajisjet në të cilat një sekuencë specifike prodhon një shërbim ose produkt (i shërben një qëllimi të caktuar biznesi) për një klient ose klientë të caktuar).

Një **aplikacion** është një paketë softuerike kompjuterike që kryen një funksion specifik për një përdorues fundor ose një aplikacion tjetër bazuar në veçori të dizajnuara me kujdes.

Një **bazë të dhënash** është një koleksion i organizuar informacioni ose të dhënash të strukturuara, të ruajtura zakonisht në mënyrë elektronike në një sistem kompjuterik.

Një **sistem operativ (OS)** është një program që vepron si një ndërfaqe ndërmjet hardëare-it të sistemit dhe përdoruesit. Për më tepër, ai trajton të gjitha ndërveprimet midis softëare-it dhe hardëare-it.

Shtresa e rrjetit punon për transmetimin e të dhënave nga një host në tjetrin të vendosur në rrjete të ndryshme.

Shtresa fizike përbëhet nga teknologjitë bazë të transmetimit të harduerit të rrjetit të një rrjeti.

IT Frameworks

- COBIT (Control Objectives for Information and related Technology)
- ISO (International Organization for Standardization)
- NIST (National Institute of Standards and Technology)
- ITIL (Information Technology Infrastructure Library)

2. Menaxhimi i rrezikut të IT-së

Risku në Sistemet e Informacionit

- Cfarë është risku?
  - “Mundësia për të pasur një impakt negativ”;
  - “Ngjarje që mund të pengojë arritjen e objektivave”;

- Tre elementët e riskut:
  - Kërcënimi (fatkeqësi natyrore, nga njeriu, teknike)
  - Impakti (matja e dëmit)
  - Probabiliteti

Vlerësimi i riskut

- Identifikimi i zonave që kanë risk të lartë
- Vlerësimi i tre elementeve të riskut: (Kërcënimi, impakti dhe probabiliteti)
- Përcaktimi i matricës së riskut

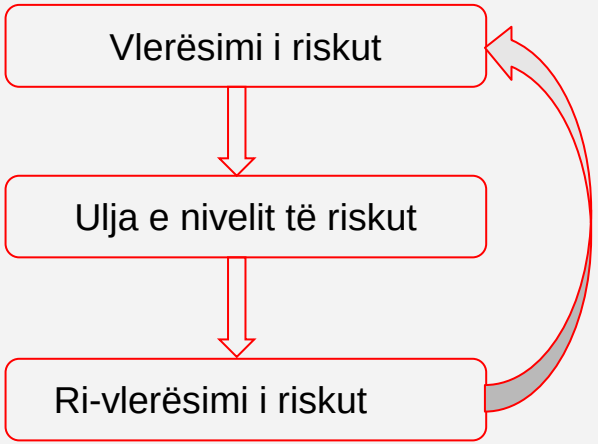
		Impakti		
		1 I ulët	**2** I mesëm	**3** I lartë
Probabiliteti	**1** I ulët			
	2 I mesëm			
	3 I lartë			

Ulja e nivelit të Riskut dhe Rivlerësimi

❖ Nënkupton uljen e riskut. **Si?**

- Implementimi i kontrolleve;
- Transferimi i riskut;
- Shmangia e riskut;

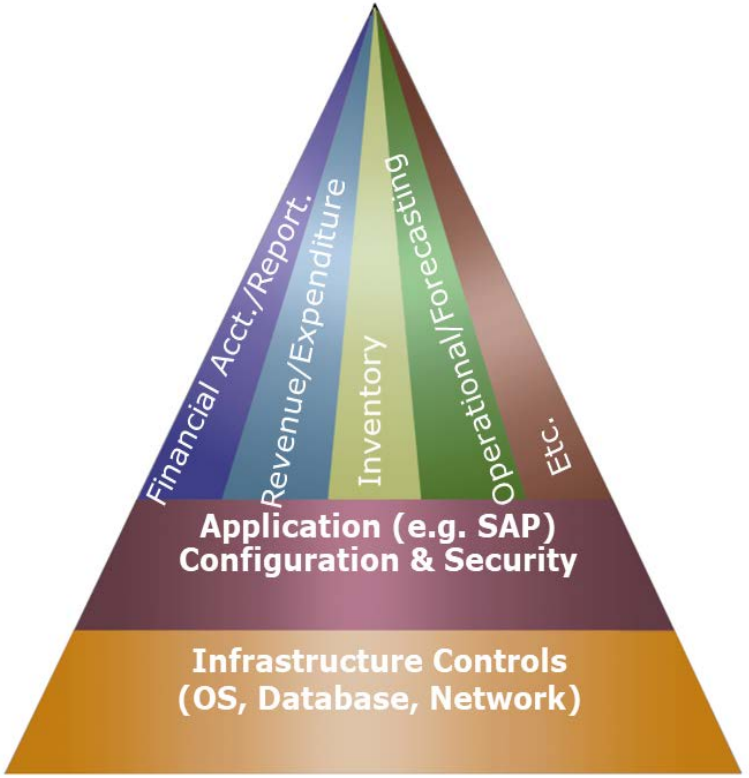
RISKU NUK MUND TË ELEMINOHET!



Çfarë mund të shkojë keq me mjedisin e IT?

Disa nga risqet e IT :

- Të dhënat janë të pasakta ose të paplota
- Regjistrimi i transaksioneve të paautorizuara ose inekzistente
- Humbje e mundshme e të dhënave ose pamundësi për të aksesuar të dhënat sipas nevojës
- Përpunimi i sistemit është i pasaktë (d.m.th., llogaritjet e pasakta)
- Logjika e raportit po zbaton ne menyre te gabuar parametrat
- Logjika e raportit po mbledh ne menyre te gabuar të dhënat burimore
- Ndryshime të paautorizuara në sistem ose programe



Rreziqet nga IT

Fusha e Kontrolleve të IT	Përshkrimi i rrezikut	Shembull rreziku nga IT
Kontrolli i ndryshimit të sistemit	Ndryshimet e Aplikimit	Ndryshime të papërshtatshme bëhen në sistemet ose programet e aplikacioneve që përmbajnë kontrolle të automatizuara përkatëse (d.m.th., cilësime të konfigurueshme, algoritme të automatizuara, llogaritje të automatizuara dhe nxjerrje të automatizuar të të dhënave) dhe/ose logjikë të raportimit.
	Ndryshimet e databazes	Ndryshime të papërshtatshme bëhen në strukturën e bazës së të dhënave dhe marrëdhëniet ndërmjet të dhënave.
	Ndryshimet e sistemeve software	Ndryshime të papërshtatshme bëhen në softuerin e sistemit (p.sh., sistemi operativ, rrjeti, softueri i menaxhimit të ndryshimeve, softveri i kontrollit të aksesit).
	Data Conversion	Të dhënat e konvertuara nga sistemet e vjetra ose versionet e mëparshme sjellin gabime të të dhënave nëse transferimi i konvertimit është i paplotë, i tepërt, i vjetëruar ose i pasaktë.

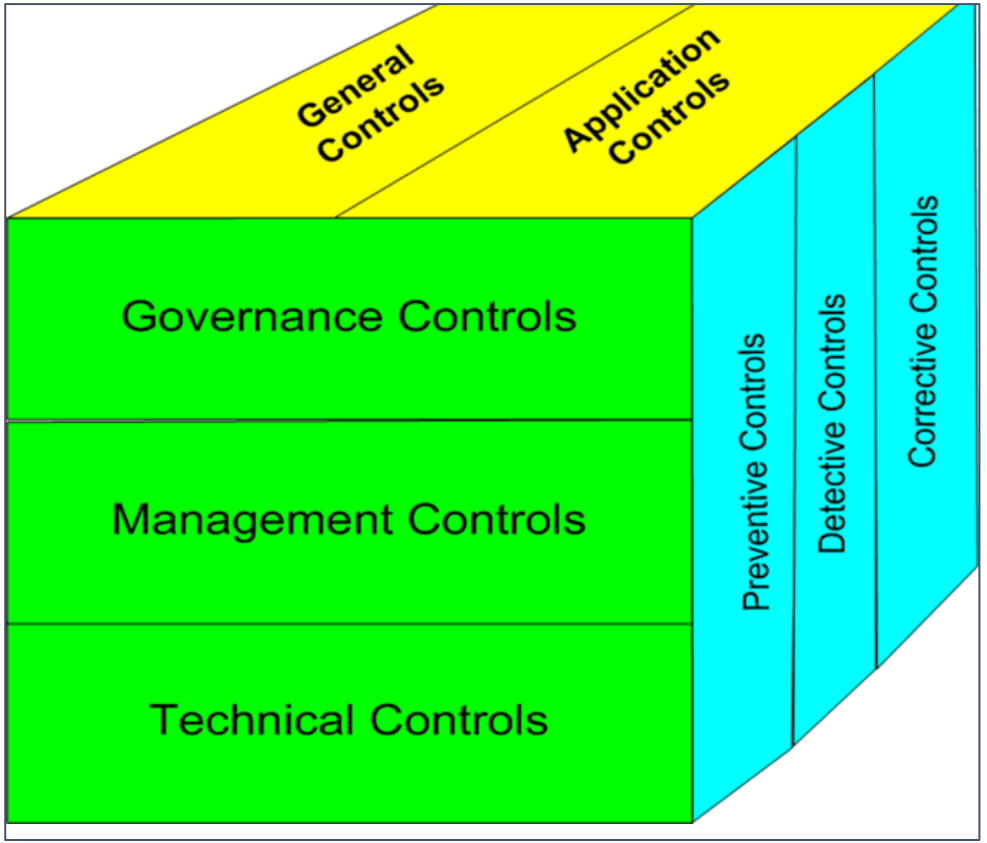
Rreziqet nga IT

Fusha e Kontrolleve të IT	Përshkrimi i rrezikut	Shembull rreziku që rrjedh nga IT
Qendra e të Dhënave dhe Operacionet e Rrjetit	Rrjeti	Rrjeti nuk parandalon në mënyrë adekuate përdoruesit e paautorizuar që të kenë akses të papërshtatshëm në sistemet e informacionit.
	Siguria fizike	Individët fitojnë akses të papërshtatshëm në pajisjet në qendrën e të dhënave dhe e shfrytëzojnë një akses të tillë për të anashkaluar kontrollet e aksesit logjik dhe për të fituar akses të papërshtatshëm në sisteme.
	Rezervimi dhe rikuperimi i të dhënave	Të dhënat financiare nuk mund të rikuperohen ose aksesohen në kohën e duhur kur ka humbje të të dhënave.
	Job scheduling	Sistemet e prodhimit, programet dhe/ose punët rezultojnë në përpunim të pasaktë, të paplotë ose të paautorizuar të të dhënave.

3.Të kuptuarit e kontrolleve të IT

Të kuptuarit e kontrolleve të IT

Kontrolli i TI-së është një proces që ofron siguri për shërbimet e informacionit dhe informacionit dhe që ndihmon në zbutjen e rreziqeve lidhen me përdorimin e teknologjisë.

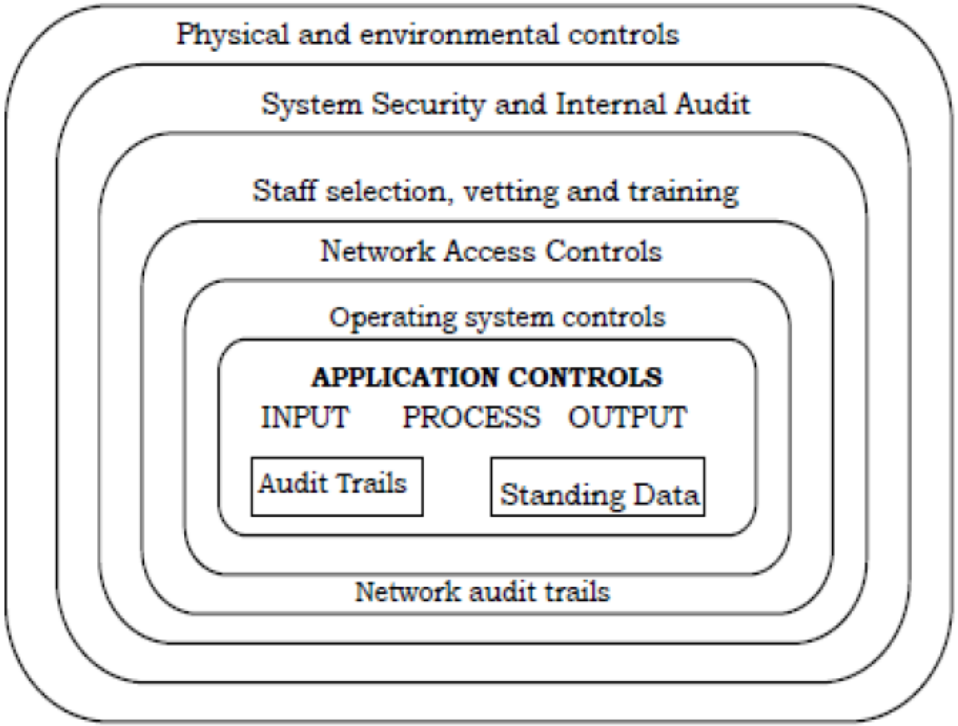


Kornizat e kontrolleve të IT

ITGC & ITAC

ITGC

ITAC



GITC – Kontrollet e Përgjithshme të Teknologjisë së Informacionit

- Qeverisja e TI-së
- Menaxhimi i sigurisë
- Menaxhimi i ndryshimeve
- Kontrolli fizik i aksesit
- Kontrollet mjedisore (shembull: datacenter)
- Vazhdimësia e shërbimit IT
- Kontrollet logjike të aksesit

ITAC – Kontrollet e Automatizuara të IT-së

Kontrollet e automatizuara janë kontrolle të krijuara për të siguruar përpunimin e plotë dhe të saktë të të dhënave.

Kontrollet e aplikimit përfshijnë:

- ➢ Kontrollet e plotësisë (Completeness checks)
- ➢ Kontrollet e vlefshmërisë (Validity checks)
- ➢ Identifikimi
- ➢ Autentifikimi
- ➢ Autorizimi
- ➢ Input Controls
- ➢ Output Controls

Të mirat e një kontrolli të përgjithshëm efektiv të teknologjisë së informacionit

- Rreziqet dhe mundësitë e reduktuara për mashtrim
- Më pak dobësi për t'u shfrytëzuar si pjesë e një shkeljeje kibernetike
- Rritja e besueshmërisë në informacionin financiar të përdorur në operacionet e biznesit, raportimin e brendshëm të menaxhimit dhe arritjen e objektivave të biznesit
- Shanse më të mëdha për të zbuluar problemet herët, përpara se ato të bëhen një problem i madh
- Pajtueshmëri më e lehtë me ligjet dhe rregulloret
- Produktiviteti rritet me kalimin e kohës
- Zvogëlohet koha për të kryer mbylljen financiare
- Avantazhi konkurrues përmes kontrolleve të përmirësuara
- Përmirësimi i vendimmarrjes së menaxhimit përmes informacionit me cilësi të lartë

4. Testimet gjatë auditimit

Testi i Projektimit dhe Zbatimit (D&I)

Qëllimi i testimit të **projektimit dhe zbatimit** të kontrolleve::

- Për të vlerësuar dizajnin e kontrolleve (pjesa e projektimit)
- Për të përcaktuar nëse kontrolli mbulon objektivin e kontrollit
- Për të konfirmuar që kontrollet janë vënë në funksion (pjesa e zbatimit)

Hapat e testimit:

- Vëzhgoni/inspektoni dhe rishikoni qasjen e kontrollit dhe testoni dizajnin për plotësinë, rëndësinë, afatin kohor dhe matshmërinë.
- Kërkoni dhe konfirmoni se përgjegjësitë për praktikën e kontrollit janë caktuar, kuptuar dhe pranuar.
- Pyetni anëtarët kryesorë të stafit për mekanizmin e kontrollit, qëllimin, llogaridhënien dhe përgjegjësinë e tij.

Vetëm kërkimi nuk është i mjaftueshëm për të vlerësuar projektimin dhe zbatimin e një kontrolli

Testi i Efektivitetit Operacional (OE)

Qëllimi i testimit të **efektivitetit operacional :**

Për të përcaktuar se masat e kontrollit të vendosura janë:

- Duke punuar sic duhet
- Në mënyrë të vazhdueshme

❖ Testuar duke marrë evidenca direkte ose indirekte për artikujt/periudhën e përzgjedhur
❖ Qasja e bazuar në kampionim

Hapat e testimit për efektivitetin operacional:

- Përcaktoni popullsinë
- Përcaktoni shpeshtësinë e aktivitetit të kontrollit
- Përcaktoni madhësinë e kampionimit
- Përcaktoni planin e testimit
- Ekzekutoni planin e testimit për çdo artikull në kampionin e zgjedhur

Si të bëjmë kampionimin e rasteve për testim?

Natyra e kontrollit	Shpeshtësia	Minimumi I madhësisë së mostrës
Manuale	Shumë herë në ditë	25
Manuale	Cdo ditë	25
Manuale	Cdo javë	5
Manuale	Cdo muaj	2
Manuale	Cdo 3- mujor	2
Automatike	Cdo vit	1
Automatike	Testoni një aplikim të çdo aktiviteti të kontrollit të programuesit (supozon se Kontrollet e Përgjithshme të IT janë efektive)	
Kontrollet e përgjithshme IT	Ndiqni udhëzimet e mësipërme për kontrollet manuale dhe të automatizuara	

Dokumentimi i testeve

Shembull i fletës së punës për dokumentimin e testit D&I dhe OE të kontrolleve

	B	C
2	**Control Objective**	**ITGC1000:** Operations are appropriately managed to support the scheduling, execution, monitoring, and continuity of IT programs and processes for the complete, accurate, and valid processing and recording of financial transactions.
3	**Control Activity**	**ITGCC100** Batch and online processing procedures are defined and executed so that jobs and/or transactions are processed to normal completion or are recovered and reprocessed.
4	**Design and Implementation Description**	We have ....
5	**Responcible persons**	
6	**Conclusion on D&I**	D&I Satisfactory
7	Gaps identified	N/A
8	**Operational Effectiveness**	
9	Nature	Manual / Automated
10	Source	
11	Frequency	Many times per day/Daily/Weekly/Monthly/Quarterly/Yearly
12	Sample size	
13	Test plan	1. 2. 3. ...
14	**Conclusion on OE**	Does NOT operate effectively
15	**Gaps**	
16	**Remediation**	
17		
18	**Evidences**	

Shembull - Menaxhimi i ndryshimeve të IT-së

Si është procesi menaxhimit të ndryshimeve të IT-së?

Në organizatat e IT-së, procesi i ndryshimit të menaxhimit zakonisht përdoret për të menaxhuar dhe kontrolluar ndryshimet në softuere, harduere dhe dokumentacion përkatës. Ndryshimi i menaxhimit është i nevojshëm kur ndikimi i një ndryshimi të pamiratuar ose aksidental mund të ketë rreziqe të rënda dhe pasoja financiare për një organizatë. Organizatat ndjekin një procedurë të përcaktuar të menaxhimit të ndryshimit e cila kërkon miratimin nga një bord përpara se të zbatohet në mjedisin operacional.

Shembull - Menaxhimi i ndryshimeve të IT-së

Objektivi i kontrollit

Procedurat formale të menaxhimit të ndryshimeve janë krijuar për të trajtuar në një mënyrë të standardizuar të gjitha kërkesat (përfshirë mirëmbajtjen dhe arnimet) për ndryshime në aplikacione, procedura, procese, parametra të sistemit dhe shërbimit, si dhe në platformat themelore.

Aktiviteti i kontrollit

Qasja për të zbatuar ndryshimet në mjedisin e aplikimit të prodhimit është e kufizuar dhe e ndarë në mënyrë të përshtatshme nga mjedisi i zhvillimit.

Tipi I kontrollit: Parandalues

Natyra e kontrollit: Manuale

Dizenjimi dhe implementimi

1. Merrni listat e aksesit të përdoruesve që kanë A) akses për të zhvilluar ndryshime në mjedisin e zhvillimit dhe B) akses për të promovuar ndryshime nga mjedisi i zhvillimit në mjedisin e prodhimit.

2. Vërtetoni që kontrollet janë zbatuar për të ndarë mjediset e prodhimit dhe zhvillimit.

Efektiviteti operacional

Frekuenca – bazuar në dukuritë / Popullsia – lista e përdoruesve të zhvilluesve

Testimi: Vëzhgoni dhe verifikoni nëse zhvilluesit kanë të njëjtat privilegje në prodhim si në mjedisin e zhvillimit.

Verifikoni nëse një akses i tillë është miratuar siç duhet nga menaxhimi.

Shembull - Menaxhimi i ndryshimeve të IT-së

Objektivi I kontrollit

Procedurat formale të menaxhimit të ndryshimeve janë krijuar për të trajtuar në një mënyrë të standardizuar të gjitha kërkesat (përfshirë mirëmbajtjen dhe arnimet) për ndryshime në aplikacione, procedura, procese, parametra të sistemit dhe shërbimit, si dhe në platformat themelore.

Aktiviteti I kontrollit

Ndryshimet miratohen dhe testohen siç duhet përpara se të zhvendosen në mjedisin e prodhimit

Tipi I kontrollit: Parandalues

Natyra e kontrollit: Manuale

Dizenjimi dhe implementimi

Për një përzgjedhje të një ndryshimi, shqyrtoni dokumentacionin mbështetës për të vlerësuar se ndryshimi është testuar dhe miratuar përpara zbatimit në sistemin e prodhimit në përputhje me planet e testimit të miratuara nga menaxhmenti.

Efektiviteti operacional

Frekuenca – bazuar në dukuritë / Popullsia – lista e ndryshimeve për periudhën e auditimit

Merrni një listë ndryshimesh të krijuara nga sistemi për periudhën e auditimit dhe kryeni procedura për të vërtetuar se evidenca është e plotë dhe e saktë. Bazuar në rrezikun që lidhet me kontrollin dhe shpeshtësinë e ndryshimeve, bëni një përzgjedhje ndryshimesh për të vlerësuar se ndryshimet janë testuar dhe miratuar përpara zbatimit në sistemin e prodhimit në përputhje me planet e testimit të miratuara nga menaxhimi

Shembull - Menaxhimi i ndryshimeve të IT-së

Objektivi I kontrollit

Procedurat formale të menaxhimit të ndryshimeve janë krijuar për të trajtuar në një mënyrë të standardizuar të gjitha kërkesat (përfshirë mirëmbajtjen dhe arnimet) për ndryshime në aplikacione, procedura, procese, parametra të sistemit dhe shërbimit, si dhe në platformat themelore.

Aktiviteti I kontrollit

Miratimi përfundimtar (autorizimi "shko/mos-shko") merret nga menaxhmenti i duhur i përdoruesve përpara se programet ose sistemet të përdoren në prodhim

Tipi I kontrollit: Parandalues

Natyra e kontrollit: Manuale

Dizenjimi dhe implementimi

1.Merrni listën e ndryshimeve për periudhën e auditimit në fushëveprim.

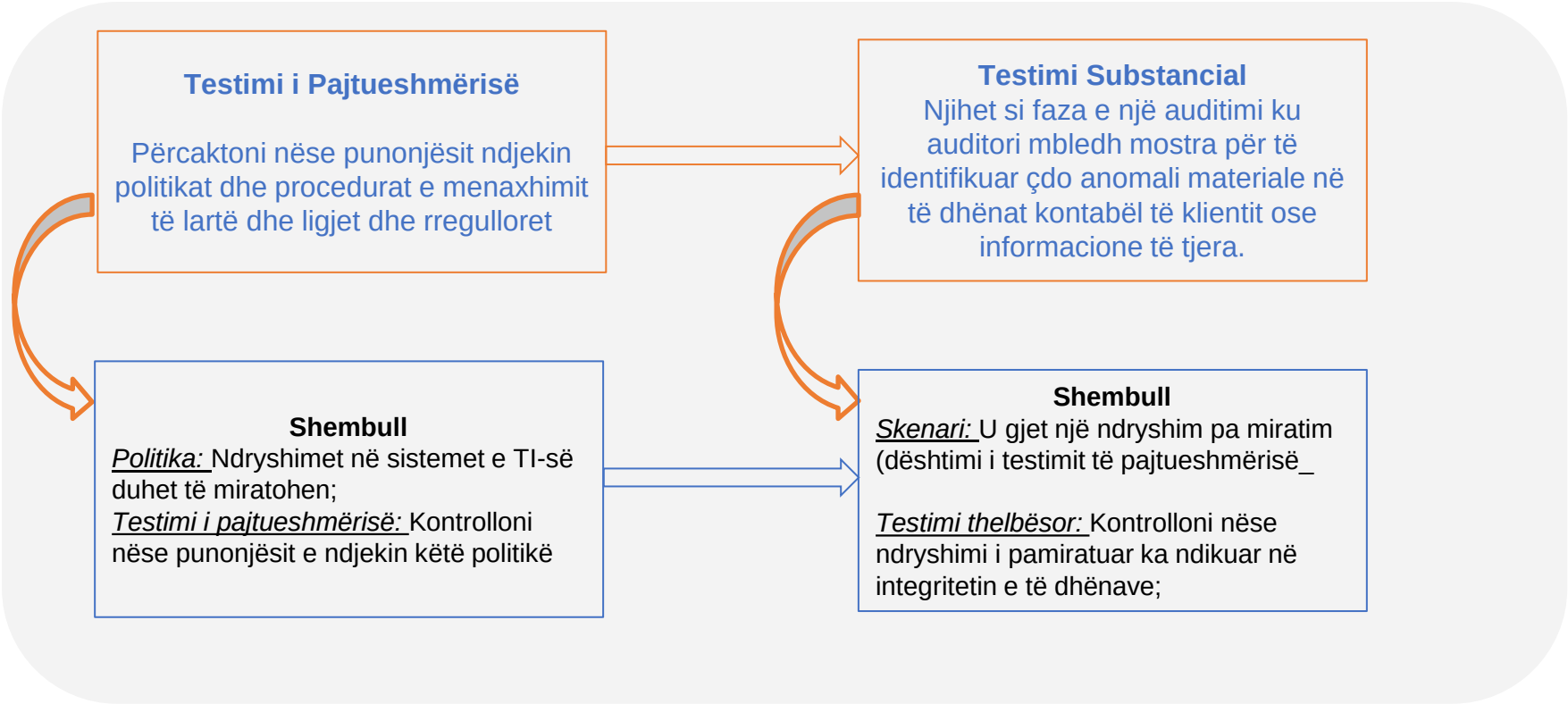
2. Për një përzgjedhje të një ndryshimi, shqyrtoni dokumentacionin mbështetës për të vlerësuar se ndryshimi ishte miratuar nga niveli i duhur i menaxhimit përpara se të zbatohej në sistemin e prodhimit.

Efektiviteti operacional

Frekuenca – bazuar në dukuritë / Popullsia – lista e ndryshimeve për periudhën e auditimit

Merrni listën e ndryshimeve për periudhën e auditimit në fushëveprim. Bazuar në rrezikun që lidhet me kontrollin dhe shpeshtësinë e ndryshimeve, bëni një përzgjedhje të ndryshimeve. Vlerësoni se ndryshimet janë miratuar nga menaxhmenti përpara zbatimit në sistemin e prodhimit në përputhje me planet e testimit të miratuara nga menaxhimi.

Shembull i testimit të përputhshmërisë dhe testimit thelbësor



5. Raportimi dhe ndjekja e rekomandimeve

Raportimi i Auditimit të IT-së

Profesionistët e auditimit dhe sigurimit të TI-së do të ofrojnë një raport për të komunikuar rezultatet pas përfundimit të angazhimit, duke përfshirë:

- Identifikimi i palëve marrëse të rapotit dhe çdo kufizim në përmbajtjen dhe qarkullimin e tij
- Qëllimi, objektivat e angazhimit, periudha e mbulimit dhe natyra, koha dhe shtrirja e punës së kryer;
- Gjetjet, përfundimet dhe rekomandimet;
- Çdo kualifikim ose kufizim në scope që ka profesionisti i auditimit dhe sigurimit të IT në lidhje me angazhimin.
- Nënshkrimi, data dhe shpërndarja sipas kushteve të statutit të auditimit ose letrës së angazhimit. Profesionistët e auditimit dhe sigurimit të IT duhet të sigurojnë që gjetjet në raportin e auditimit të mbështeten nga dëshmi të mjaftueshme, të besueshme dhe relevante.

Aktivitete Follow Up

- Një proces nëpërmjet të cilit auditorët e brendshëm vlerësojnë përshtatshmërinë, efektivitetin dhe afatin kohor të veprimeve të ndërmarra nga menaxhmenti mbi vëzhgimet dhe rekomandimet e raportuara, duke përfshirë ato të bëra nga auditorët e jashtëm dhe të tjerë.
- Duhet të krijohet një proces vijues për të ndihmuar në sigurimin e arsyeshëm që çdo rishikim i kryer nga profesionistët i ofron përfitim optimal kompanisë duke kërkuar që rezultatet e dakorduara që dalin nga rishikimet të zbatohen në përputhje me angazhimint e menaxhimit ose që menaxhmenti (ekzekutiv) të njohë dhe pranojë rrezikun e vonesës ose moszbatimit të rezultateve dhe/ose rekomandimeve të propozuara.

Kjo guide është realizuar në kuadër të projektit ***“Edukimi profesional i të rinjve studentë në fushën e auditimit të brendshëm dhe të sistemeve të teknologjisë së informacionit”*** *i zhvilluar me mbështetjen e Kongresit Rinor Kombëtar në bashkëpunim me Bashkia Tiranë në kuadër të “Tirana EYC 2022" Tirana European Youth Capital 2022, në kuadër të programit “Rinia prodhon Ekonomi Krijuese dhe Novative”.*