PEMPAL

Zajednica prakse za unutarnju reviziju (IACOP)
REVIZIJA IT-a: od teorije do prakse
WEBINAR

Resursi za reviziju IT-a i njezino planiranje

Profesor Frank Yam

Predsjednik Upravnog odbora i glavni izvršni direktor društva Focus Strategic Group Inc

23. studenoga/novembra 2020.

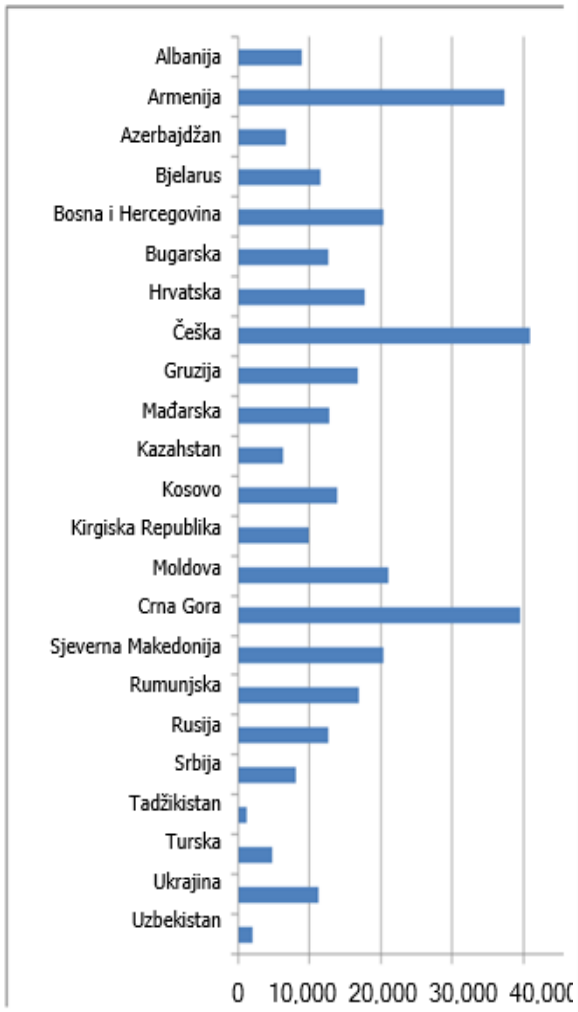
Sadržaj

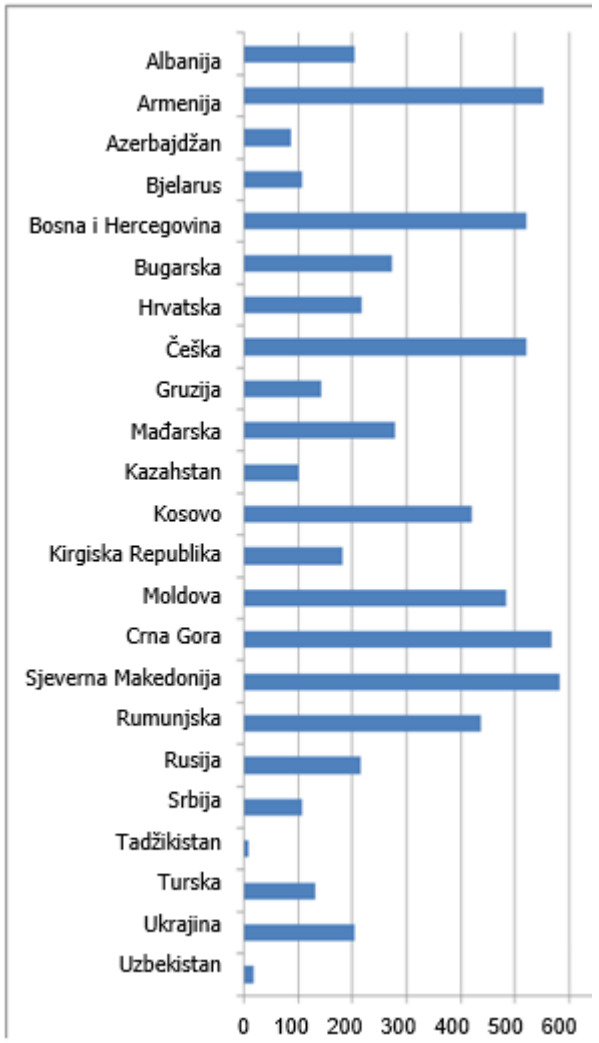
- **Prihvaćanje novonastale situacije (tzv. novo normalno)**
  - COVID-19
  - Utjecaj na funkcije unutarnje revizije
  - Sve postaje digitalno
- **Resursi za reviziju IT-a**
- **Planiranje revizije IT-a**

NOVONASTALA SITUACIJA

nakon pandemije koronavirusne bolesti (COVID-19)

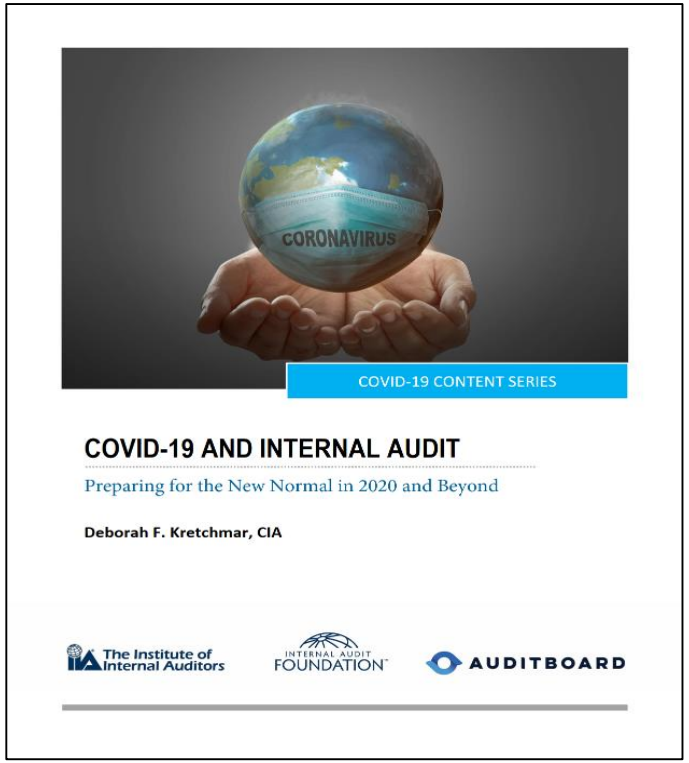
Zemlja	Stanovništvo	Broj potvrđenih slučajeva/1M	Broj smrtnih slučajeva/1M
Albanija	2.876.641	8.969	205
Armenija	2.965.275	37.281	552
Azerbajdžan	10.172.439	6.743	87
Bjelarus	9.448.180	11.574	108
Bosna i Hercegovina	3.273.270	20.336	520
Bugarska	6.929.071	12.601	274
Hrvatska	4.095.903	17.784	218
Češka	10.716.269	40.948	520
Gruzija	3.986.347	16.697	142
Mađarska	9.651.311	12.730	279
Kazahstan	18.858.176	6.283	101
Kosovo	1.810.366	13.934	421
Kirgiska Republika	6.563.032	9.806	181
Moldova	4.030.509	21.016	484
Crna Gora	628.095	39.588	567
Sjeverna Makedonija	2.083.343	20.419	582
Rumunjska	19.190.198	16.889	437
Rusija	145.957.452	12.586	216
Srbija	8.724.381	8.072	107
Tadžikistan	9.614.381	1.192	9
Turska	84.668.717	4.749	132
Ukrajina	43.636.591	11.225	205
Uzbekistan	33.644.633	2.061	18
PROSJECNO	19.283.677	15.369	277





NOVONASTALA SITUACIJA

Utjecaj pandemije koronavirusne bolesti (COVID-19) na funkcije unutarnje revizije



Glavna pitanja koja su premalo zastupljena u godišnjim planovima revizije:

1) **Kibernetička sigurnost**
   - Organizacije su svojim djelatnicima omogućile rad s različitih lokacija, pri čemu se oslanjaju na procese i kontrole nad kibernetičkim rizicima koji možda nisu adekvatno ocijenjeni.

2) **Informacijska tehnologija**
   - Gotovo 60% organizacija primjenilo je novu tehnologiju i sigurnost podataka

3) **Odnosi s trećim stranama**
   - Manje od polovine (48%) organizacija izdvojilo je resurse UR-a za odnose s trećim stranama

MEĐUTIM, NIJE SAMO RIJEČ O KORONAVIRUSNOJ BOLESTI

NOVONASTALA SITUACIJA

Sve postaje digitalno

Za organizacije:

- Djelatnici mogu raditi s različitih lokacija
- Fleksibilno radno vrijeme
- Ujednačeni rasporedi
- Osiguravanje OZO-a djelatnicima (čak i klijentima i gostima)
- Prioritet su (1) sigurnost svih osoba i (2) CEM i BCP
- Nove strategije i inicijative (uključujući one povezane s tehnologijom)
- Mogući otkazi

Za unutarnje revizore:

- Revizija na daljinu (telekonferencije, dijeljenje zaslona, videokonferencije, dijeljenje datoteka)
- Promjena vještina koje su potrebne kao posljedica digitalne transformacije
- Nezaposlenost i ekonomska kriza povećat će rizike od prijevare (stoga se i fokus revizije mora promijeniti)

Resursi za reviziju IT-a

Tko nam je potreban?

KLJUČ uspjeha = izgradnja timova koji mogu biti uspješni u budućnosti koju nije moguće predvidjeti

Stoga, nastavite se osnaživati!

Izvor: Video „Koje će vještine revizor trebati u budućnosti?" (CA - A/NZ)

Resursi za reviziju IT-a

Tko nam je potreban?

- Umjetna inteligencija
- Strojno učenje
- Veliki podaci
- RPA
- Lanac blokova
- DevSecOps
- Agile / SCRUM
- Digitalna transformacija
- Ekosustav
- UI / UX
- Razmišljanje o dizajnu
- Računalstvo u oblaku
- SaaS, IaaS, PaaS
- VPN
- API
- SDK
- Kvantno računalstvo
- Nanotehnologija
- Disruptivne tehnologije
- SOC

Osobe koje mogu razumjeti izazove u poslovanju i usklađivanju IT-a

- Zoom
- Webex (Cisco)
- Teams (MS)
- Meet (Google)
- KOL
- IoT
- VR / AR
- 5G
- FinTech, RegTech, EdTech, HealthTech
- Kriptovaluta
- e-Novčanici
- e-Plaćanja
- QR kodovi
- Dronovi
- Chatboti
- 3D printanje
- Nosiva tehnologija
- Gospodarstvo temeljeno na honorarnom radu
- Pametni gradovi/pametne vlade
- Milenijalci

Resursi za reviziju IT-a

Tko?

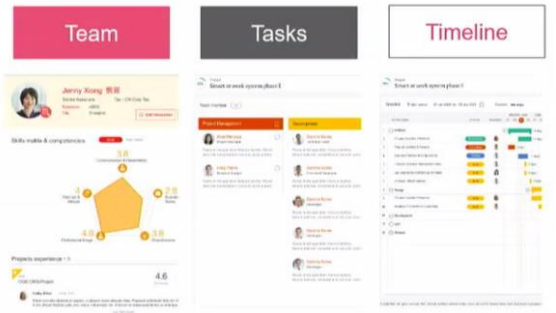
- **Stalno zaposleni revizori**
  - Hitna potreba za poboljšanjem vještina i stjecanjem novih vještina
  - Razmotriti privremene premještaje
  - Razmjena najboljih praksi

- **Suradnja**
  - Poštovanje propisa
  - Unutarnja kontrola
  - Upravljanje rizicima
  - Sigurnost
  - Privatnost
  - Istraživanje prijevare
  - Vanjska revizija

- **Djelomična eksternalizacija određenih funkcija**
  - Tehnička područja
  - Povremeno, prema potrebi
  - Prijenos znanja

Resursi za reviziju IT-a

Kako?



Upravljanje revizorima

RPA / CAAT

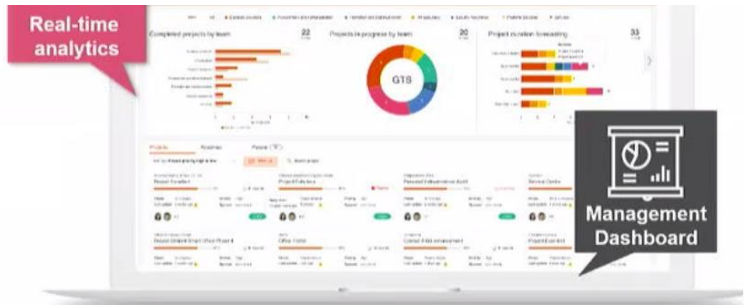
Upravljanje subjektima revizije

Upravljanje portfeljima

Upravljanje projektima

Upravljanje rizicima (i planiranje)

Upravljanje radnim dokumentima



Planiranje revizije IT-a

Komponenta sustava upravljanja	Primjeri portfelja revizije IT-a	Potencijalni izvor
Procesi	Procesi COBIT® 2019.	C06IT 2019 Ciljevi upravljanja i rukovodstva[1,2]
Organizacijske strukture	Dobavljači treće strane, podružnice, odjeli poduzeća	Sustav planiranja resursa poduzeća (ERP), dokumentiranje strukture poduzeća, organizacijske tablice
Načela, politike, procedure	Privatnost, zakoni, propisi i drugi zahtjevi u pogledu poštovanja propisa	Pravne funkcije, funkcije privatnosti, sigurnosti i upravljanja te rizika i poštovanja propisa (GRC)
Informacije	Način na koji revizija IT-a izvještava o svojim rezultatima rada	Zahtjevi revizorskog odbora
Kultura, etika i ponašanje	Kontrole preporuka revizije, nove inicijative u pogledu IT-a	Datumi završetka provedbe preporuka unutarnje revizije i rukovodstva, provedene preporuke
Djelatnici, vještine i sposobnosti	Obuka koju trebaju proći revizori IT-a, obuka koju trebaju održati revizori IT-a, obuka na temu općenite svijesti o IT-u	Planovi obuke, planovi osobnog razvoja
Usluge, infrastruktura i aplikacije	Aplikacije, baze podataka, internetske stranice, operativni sustavi, virtualni strojevi itd.	Registar imovine IT-a

Izvor: Glasilo ISACA-e – 1. svibnja/maja 2019. – „Razvoj plana revizije IT-a s pomoću okvira COBIT 2019”

Planiranje revizije IT-a

Planiranje na godišnjoj razini

- Razmotrite usvajanje pristupa temeljenog na **agilnom upravljanju portfeljima**
  - Prihvatite kratkoročne prioritete
  - Redoviti pregledi/ažuriranje plana revizije (kako bi odražavali promjenu tempa u pogledu rizika i potreba za pružanjem uvjerenja)
- Omogućite **povećanu fleksibilnost** plana revizije:
  - Nastojite pomoći s **novim projektima / inicijativama**
  - Sada je najbolje vrijeme za izgradnju odnosa i dokazivanje vrijednosti UR-a
- **Surađujte s ključnim zainteresiranim stranama** (uključujući revizorski odbor) kako biste razumjeli sve nove i / ili povećane rizike i procijenili kako najbolje podržati pružanje uvjerenja
- Povećajte broj sastanaka na temu postignutog napretka koje održavate s ključnim zainteresiranim stranama u različitim djelatnostima. Kada je to moguće, služite se videopozivima kako biste **izgradili odnos i stekli povjerenje**.

Planiranje revizije IT-a

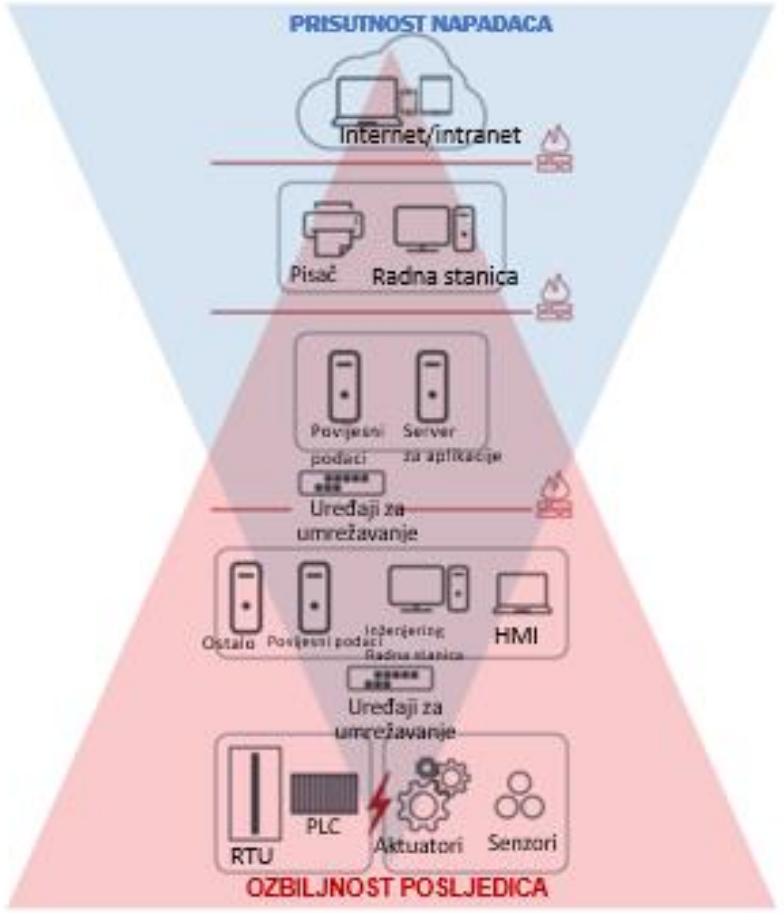
Planiranje na godišnjoj razini – predložena područja za fokus

(1) Kibernetička sigurnost (ucjenjivački softver, kibernetičke ucjene)

- Kontrole pristupa korisnika
- Sigurnosna kopija i oporavak podataka
- Regulatorni zahtjevi u pogledu privatnosti podataka (GDPR itd.)

Ucjenjivački softver - sprječava vam pristup podacima

Cyber Extortion - A threat to make your data public to others

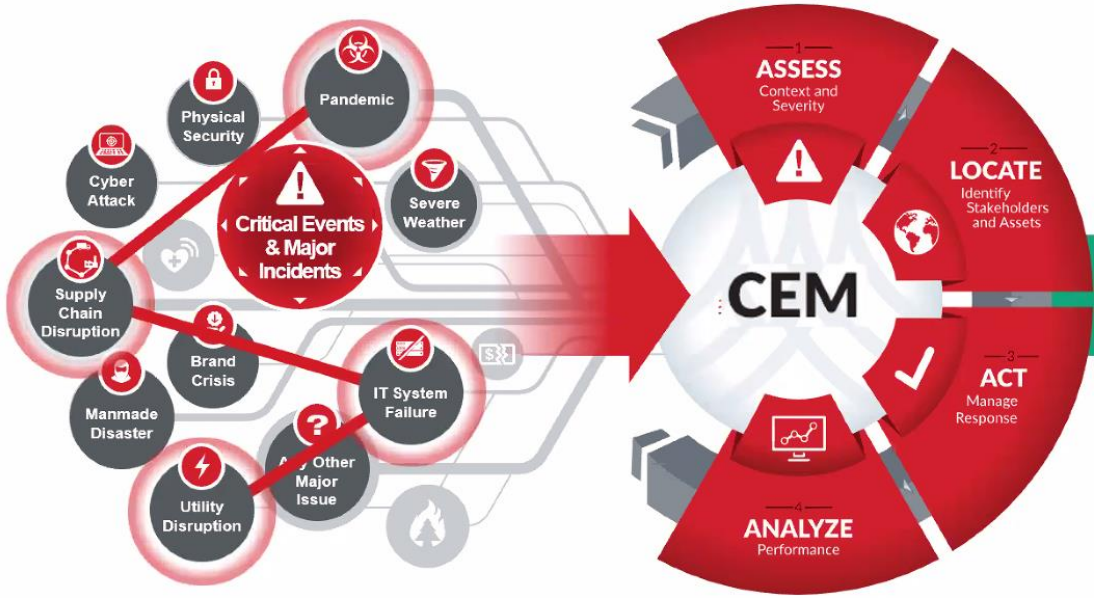


Planiranje revizije IT-a

Planiranje na godišnjoj razini – predložena područja za fokus

(2) Kontinuitet poslovanja

- ☐ Plan za oporavak podataka (CEM)
- ☐ Segregacija kritičnih timova (u slučaju karantene)
- ☐ Pregled digitalnih mogućnosti od transakcija do interakcija s klijentima
- ☐ Ponovno razmotrite analizu utjecaja na poslovanje (BIA) i „najgore scenarije”
- ☐ Planovi za upravljanje medijima



(3) Pregledajte IT procese kojima NE upravlja IT

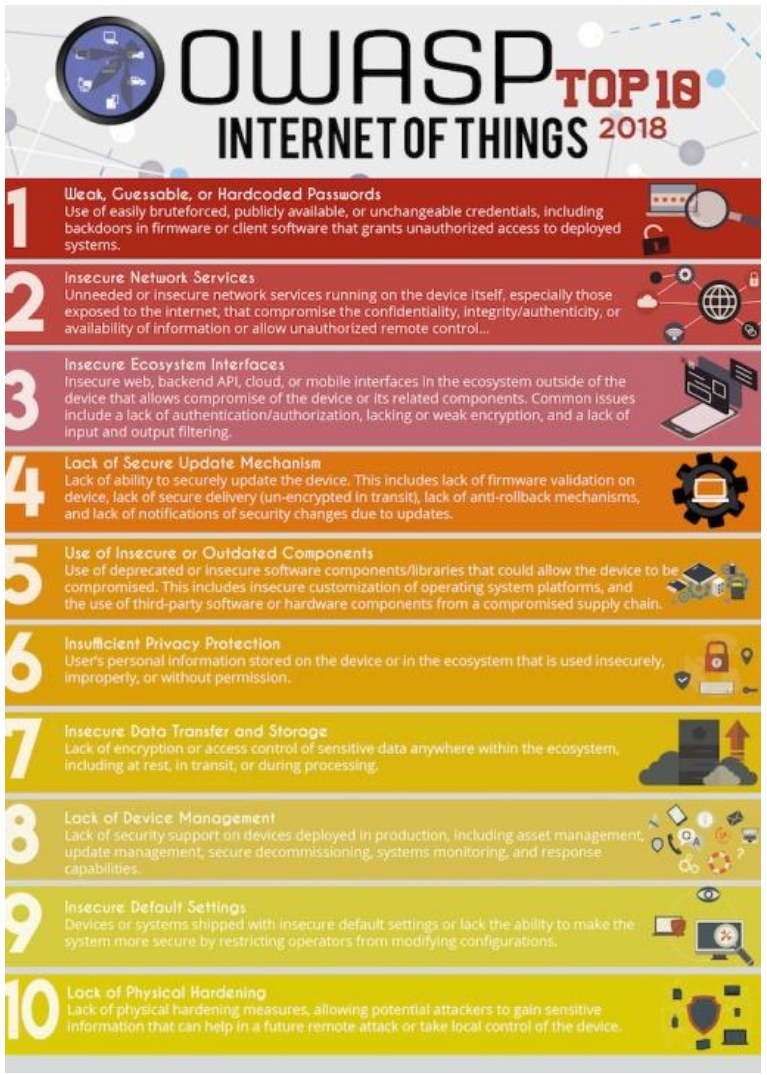
(4) Pregledajte postojeće politike, smjernice

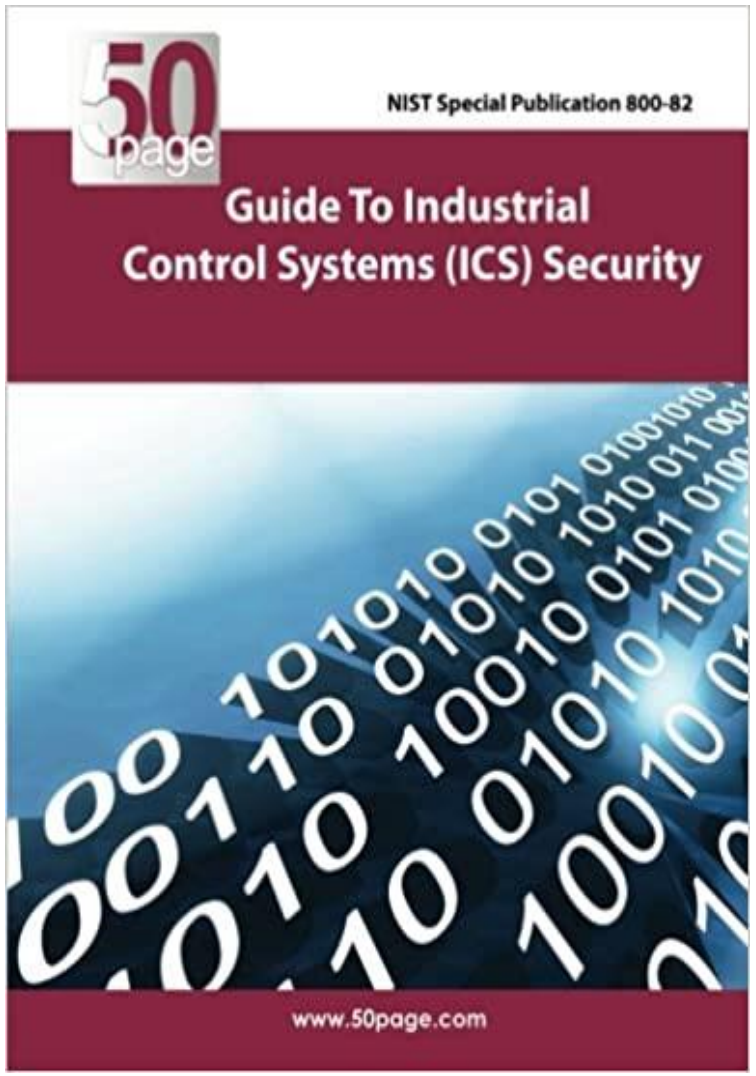
Planiranje revizije IT-a
Planiranje angažmana

Predložena područja fokusa:

- Izvedivost revizije na daljinu
- Dostupnost elektroničke dokumentacije (+ mogućnost skeniranja dokumenata)
- Pojašnjenja na daljinu, novosti o napretku i izvještaji o nalazima u nastanku
- Dostupnost novih tehnologija za isporuku posla, kao što su Microsoft Teams, Zoom ili Skype za virtualne sastanke / radionice (razmotrite snimanje takvih interakcija kako biste poboljšali dokaze o učinku UR-a).
- Primjena analitike radi povećanja obuhvata i fokus na iznimke
- Zaobilaženje kontrola (djelatnici koji nastoje otkriti kako zaobići postojeće kontrole zbog nesigurnosti)
- Povećani rizici od prijevare

Korisni resursi za reviziju IT-a





Što je sljedeće

- **Revizori**
  - Procijenite prikladnost svojih vještina (u pogledu budućnosti)
- **Voditelji revizija**
  - Uložite u RPA i umjetnu inteligenciju
  - Zaposlite i obučite djelatnike koji vladaju tehnologijom
- **Vlade / organizacije**
  - Pripremite se na dramatične promjene u načinu rada i raspodjeli radne snage
  - Prihvatite tehnologiju i digitalnu transformaciju
  - Fokusirajte se na UI / UX

Nitko ne zna kakva će biti digitalna budućnost …

HVALA!