

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**

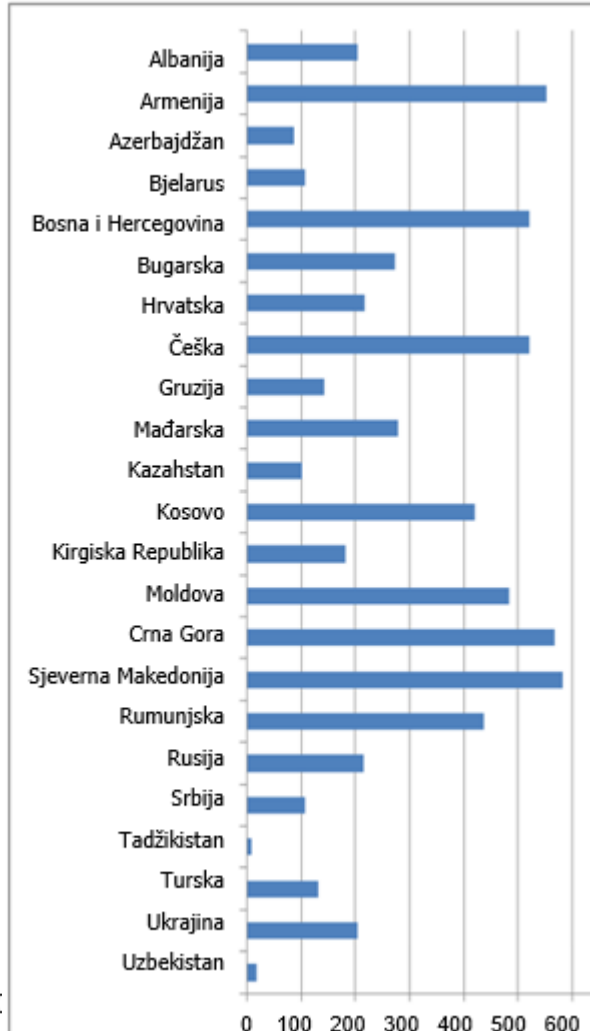
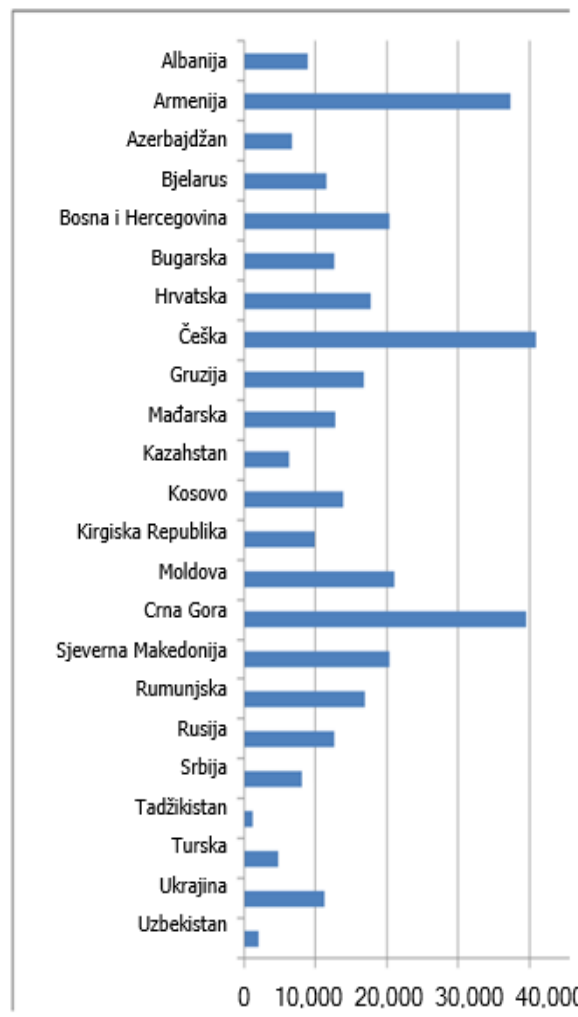
- ❑ **Prihvatanje novonastale situacije (tzv. novo normalno)**
 - ❑ COVID-19
 - ❑ Utjecaj na funkcije unutarnje revizije
 - ❑ Sve postaje digitalno
- ❑ **Resursi za reviziju IT-a**
- ❑ **Planiranje revizije IT-a**

NOVONASTALA SITUACIJA

nakon pandemije koronavirusne bolesti (COVID-19)

Zemlja
Albanija
Armenija
Azerbajdžan
Bjelarus
Bosna i Hercegovina
Bugarska
Hrvatska
Češka
Gruzija
Mađarska
Kazahstan
Kosovo
Kirgiska Republika
Moldova
Crna Gora
Sjeverna Makedonija
Rumunjska
Rusija
Srbija
Tadžikistan
Turska
Ukrajina
Uzbekistan
PROSJEČNO

Stanovništvo	Broj potvrđenih slučajeva/1M	Broj smrtnih slučajeva/1M
<u>2.876.641</u>	8.969	205
<u>2.965.275</u>	37.281	552
<u>10.172.439</u>	6.743	87
<u>9.448.180</u>	11.574	108
<u>3.273.270</u>	20.336	520
<u>6.929.071</u>	12.601	274
<u>4.095.903</u>	17.784	218
<u>10.716.269</u>	40.948	520
<u>3.986.347</u>	16.697	142
<u>9.651.311</u>	12.730	279
<u>18.858.176</u>	6.283	101
<u>1.810.366</u>	13.934	421
<u>6.563.032</u>	9.806	181
<u>4.030.509</u>	21.016	484
<u>628.095</u>	39.588	567
<u>2.083.343</u>	20.419	582
<u>19.190.198</u>	16.889	437
<u>145.957.452</u>	12.586	216
<u>8.724.381</u>	8.072	107
<u>9.614.381</u>	1.192	9
<u>84.668.717</u>	4.749	132
<u>43.636.591</u>	11.225	205
<u>33.644.633</u>	2.061	18
19.283.677	15.369	277



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



COVID-19 AND INTERNAL AUDIT

Preparing for the New Normal in 2020 and Beyond

Deborah F. Kretchmar, CIA



Glavna pitanja koja su premalo zastupljena u godišnjim planovima revizije:

1) Kibernetička sigurnost

- Organizacije su svojim djelatnicima omogućile **rad s različitim 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

5

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?

6



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?

7

- 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

TRENDOVI U DIGITALNOJ TEHNOLOGIJI



KULTUROLOŠKI TRENDOVI



UTJECAJ NA POSLOVANJE I FUNKCIJU IT-a

Dvomodalni IT | Pomoćni IT | Pristup temeljen na izgradnji odnosa | Agilnost i fleksibilnost | Međuorganizacijska suradnja | Pobošanje vještna | Izloženost novom riziku

DIGITALNA TRANSFORMACIJA = PONOVNO OSMIŠLJAVANJE POSLOVNOG MODELA + (NOVACIJA U TEHNOLOGIJI (PRIMJERENA))

DIGITALIZACIJA S RPA-om = POBOLJŠAVANJE POSLOVNIH PROCESA + AUTOMATIZACIJA (LIČNKOVITOST I EFIKASNOST)

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

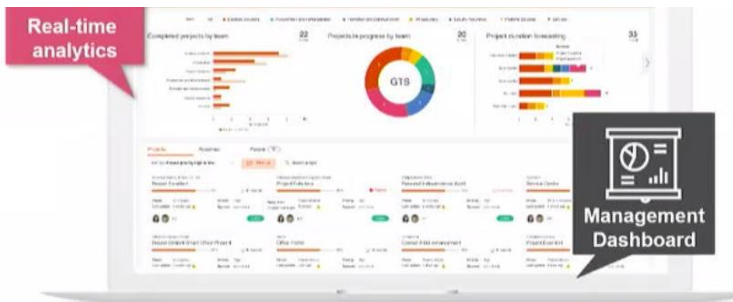
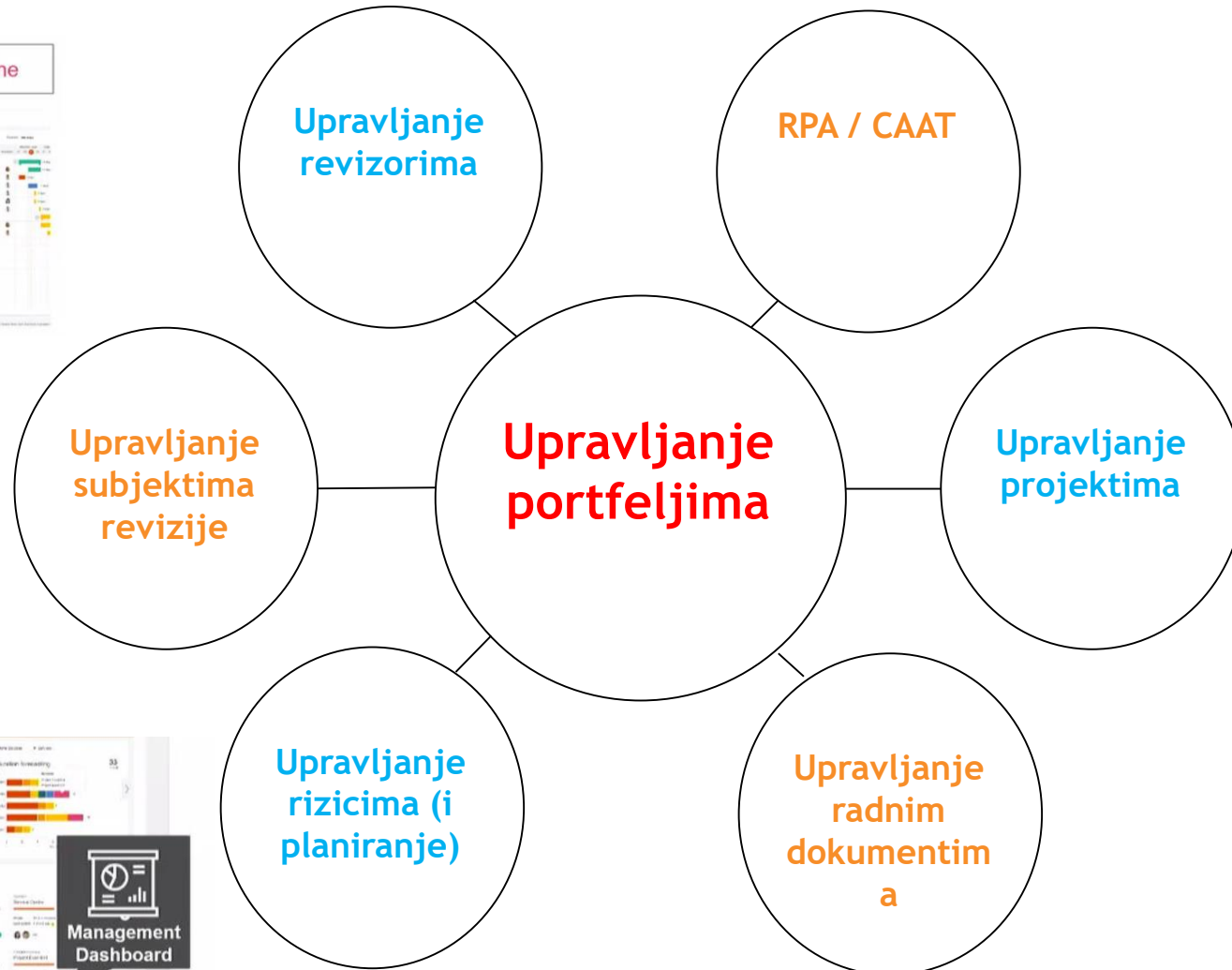
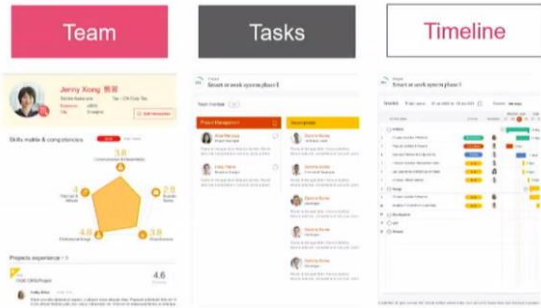
❑ **Djelomična eksternalizacija određenih funkcija**

- ❑ Tehnička područja
- ❑ Povremeno, prema potrebi
- ❑ Prijenos znanja



Resursi za reviziju IT-a

Kako?



Planiranje revizije IT-a



Komponenta sustava upravljanja	Primjeri portfelja revizije IT-a	Potencijalni izvor
Procesi	Procesi COBIT® 2019.	COBIT 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 revizorskoj 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

Planiranje revizije IT-a

Planiranje na godišnjoj razini

11

- ❑ 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
- ❑ **Suradujte 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

12

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

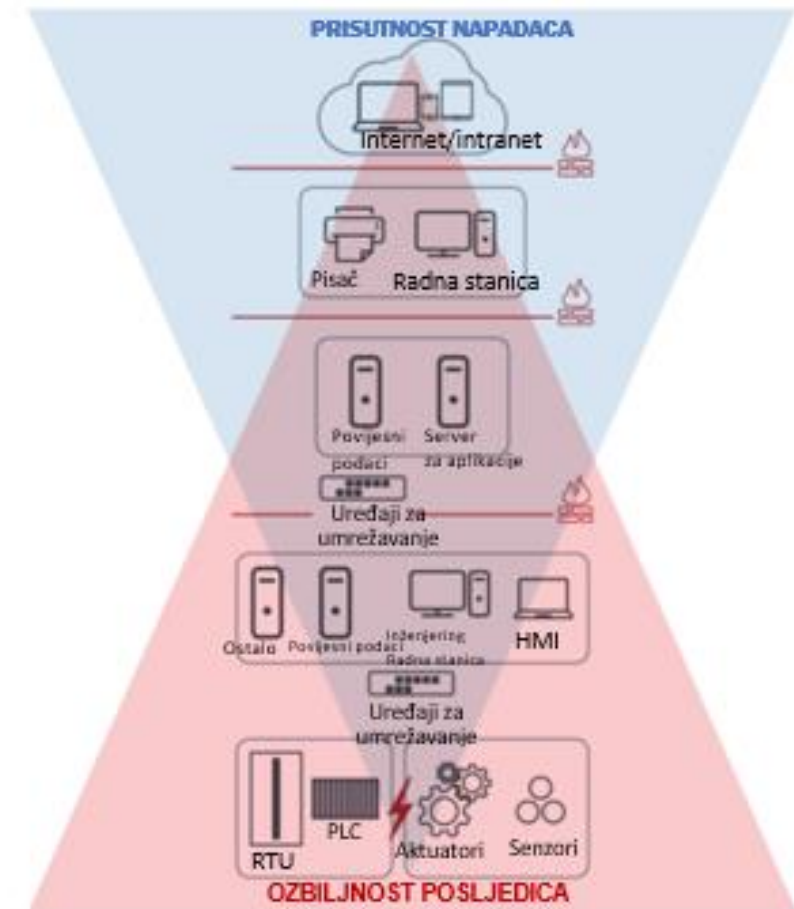
- Kontrole pristupa korisnika
- Sigurnosna kopija i oporavak podataka
- Regulatorni zahtjevi u pogledu privatnosti podataka (GDPR itd.)



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

13

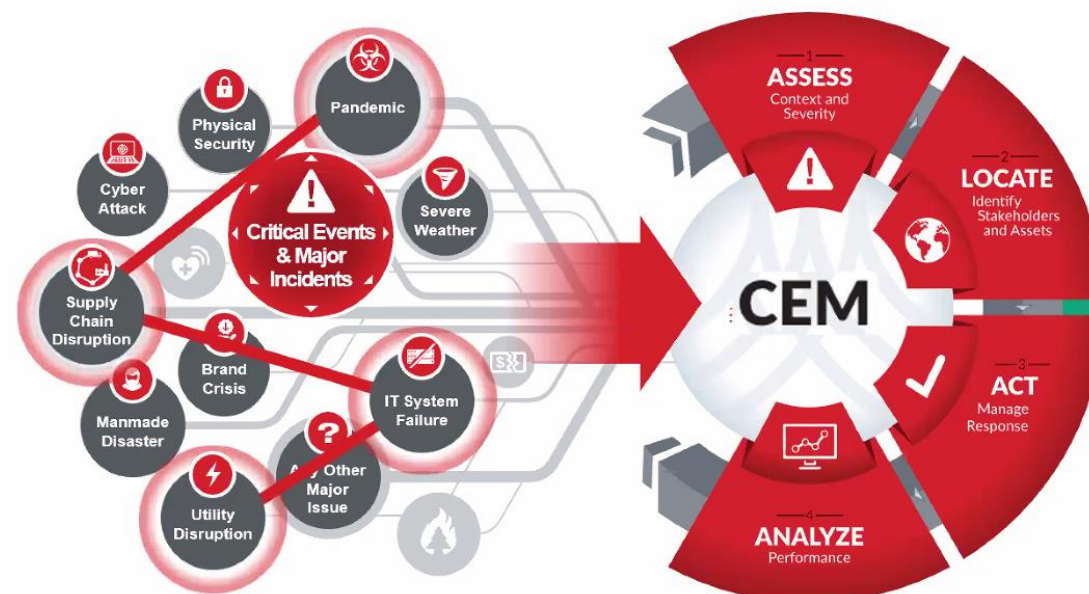
(2) Kontinuitet poslovanja

- 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
- ❑ Zaobilazjenje kontrola (djelatnici koji nastoje otkriti kako zaobići postojeće kontrole zbog nesigurnosti)
- ❑ Povećani rizici od prijevare

Korisni resursi za reviziju IT-a

NIST Cyber Security Framework



OWASP TOP 10 INTERNET OF THINGS 2018

- Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.
- Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...
- Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
- Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
- Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
- Insufficient Privacy Protection**
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
- Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
- Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
- Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
- Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

50
page

NIST Special Publication 800-82

Guide To Industrial Control Systems (ICS) Security

www.50page.com

Što je sljedeće

16

❑ Revizori

- ❑ Procijenite prikladnost svojih vještina (u pogledu budućnosti)

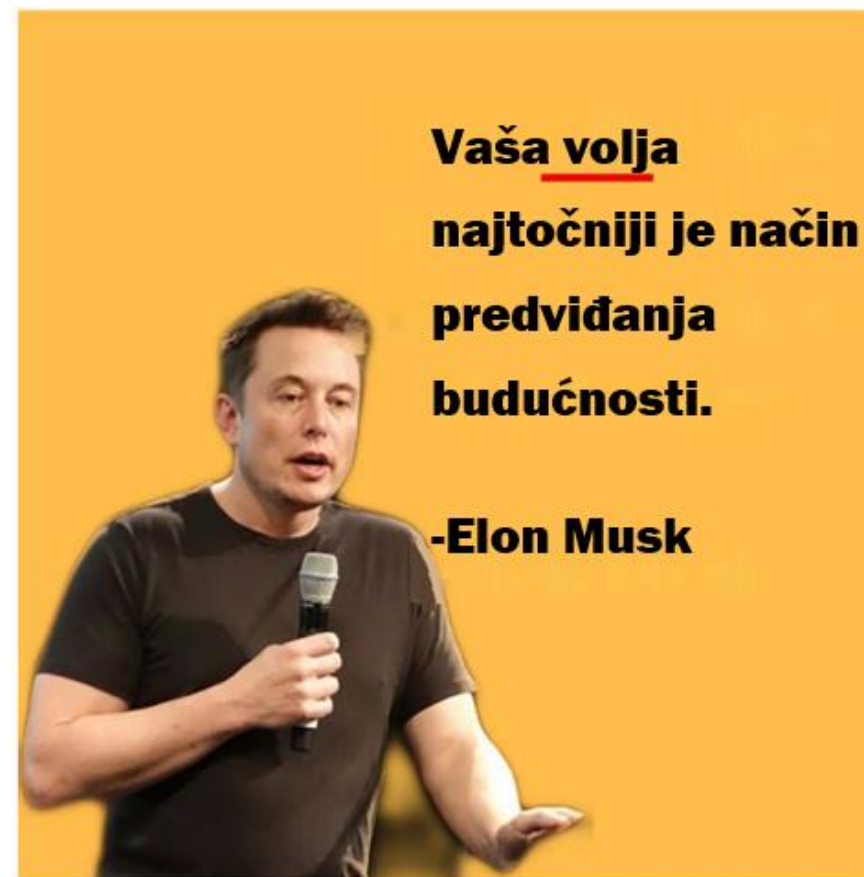
❑ Voditelji revizija

- ❑ 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!
