Vladaiprijatelji Caffe 8

Šta je novo - ISO 27001&ISO 27002 ?

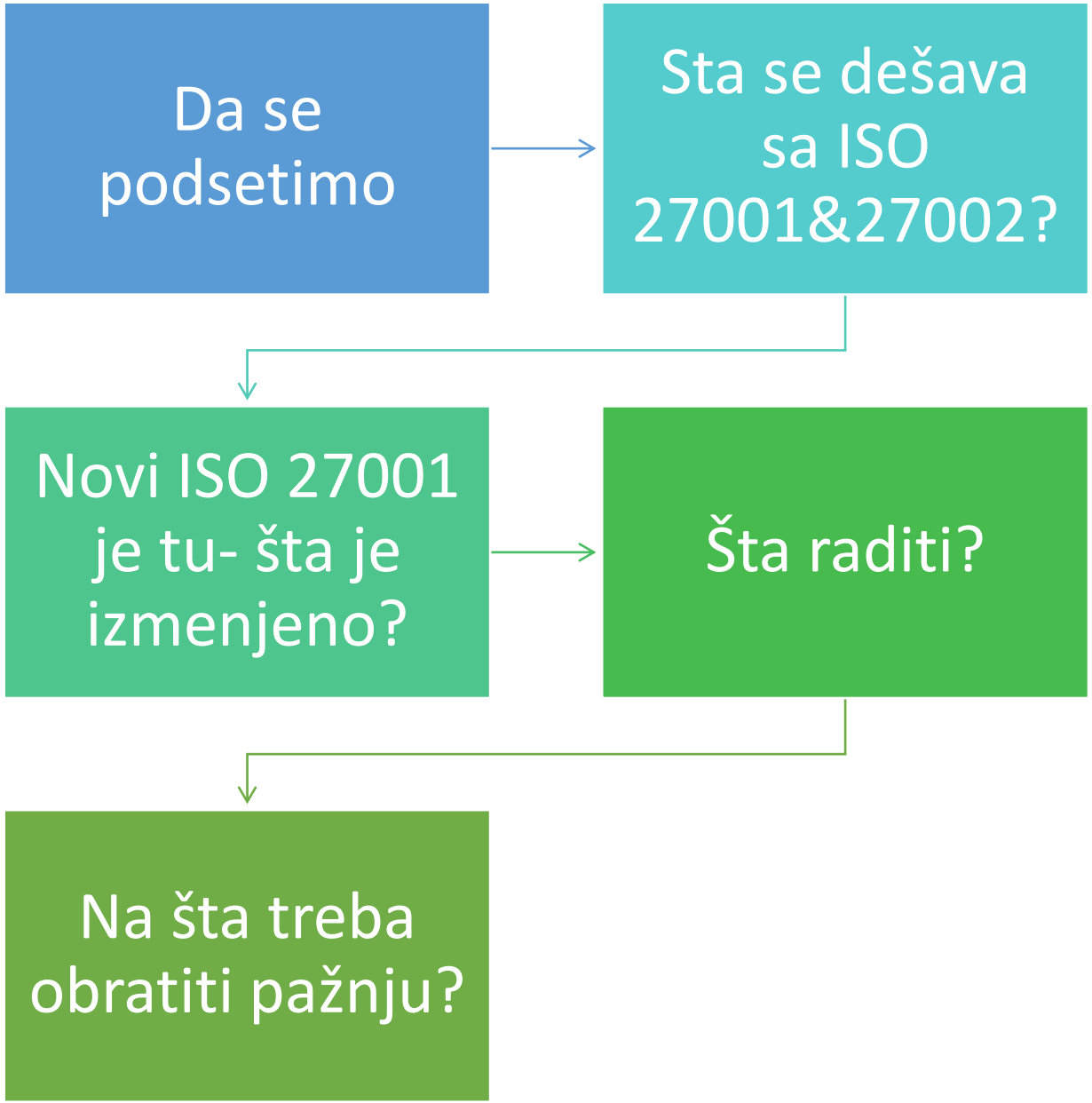
29 April 2022 u 12 h.

Literatura / video prilozi

1. https://bestpractice.biz/changes-to-iso-27001-in-2022/
2. https://www.pivotpointsecurity.com/blog/what-the-new-iso-270012021-release-will-mean-to-you/
3. https://www.stickmancyber.com/cybersecurity-blog/10-most-common-questions-about-the-2022-update-to-iso-270012013
4. https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates
5. https://subtelforum.com/stf-mag-feature-iso-270012022-is-coming-what-do-the-changes-mean-for-you/
6. https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/

1. www.youtube.com/watch?v=tWyuEiXVHnY
2. https://www.youtube.com/watch?v=kqQyqZz0C48
3. https://www.youtube.com/watch?v=7hBDeHTp-2w
4. https://www.youtube.com/watch?v=FeBLZ7P4mFA

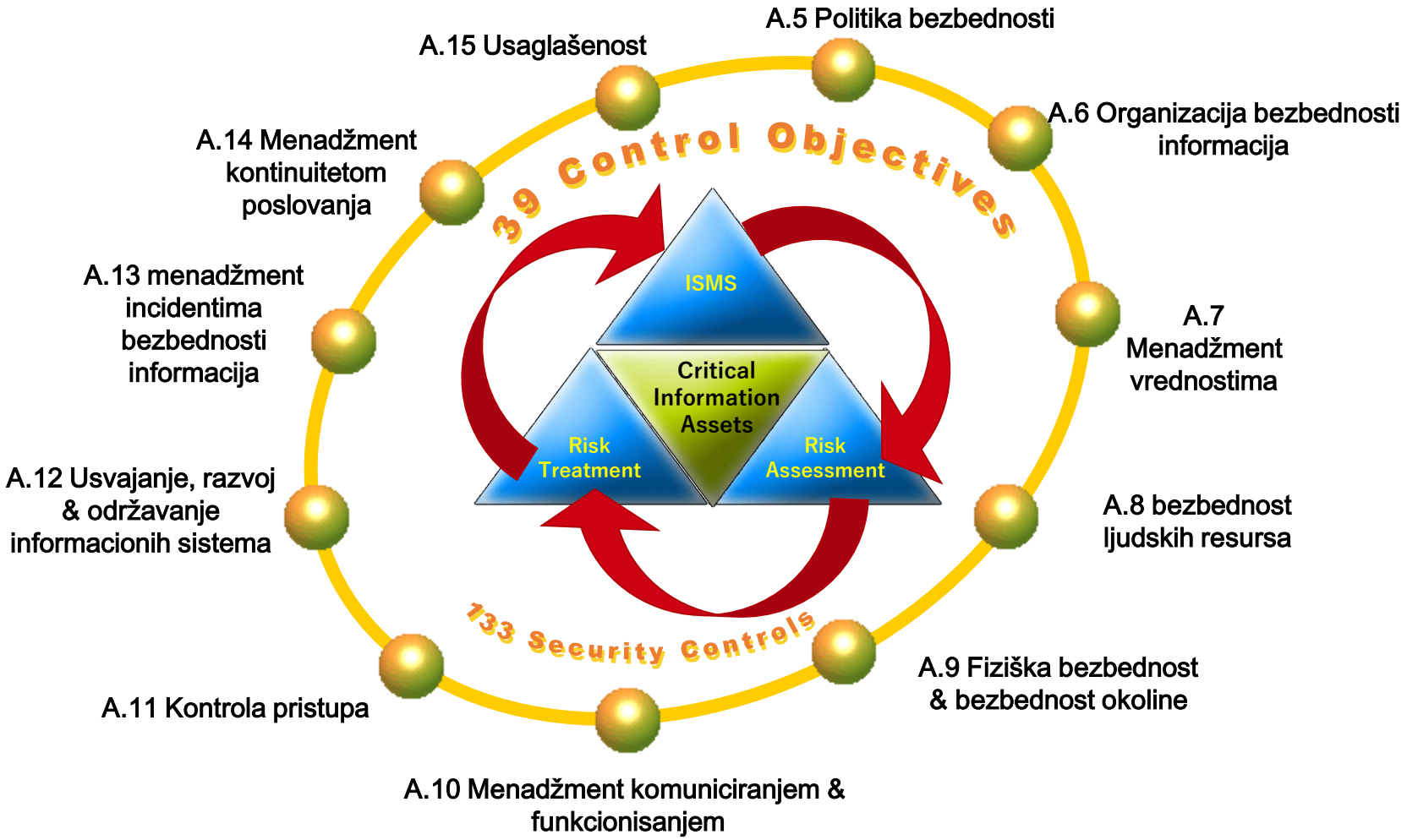
Šta se u uvodu prikazuje?



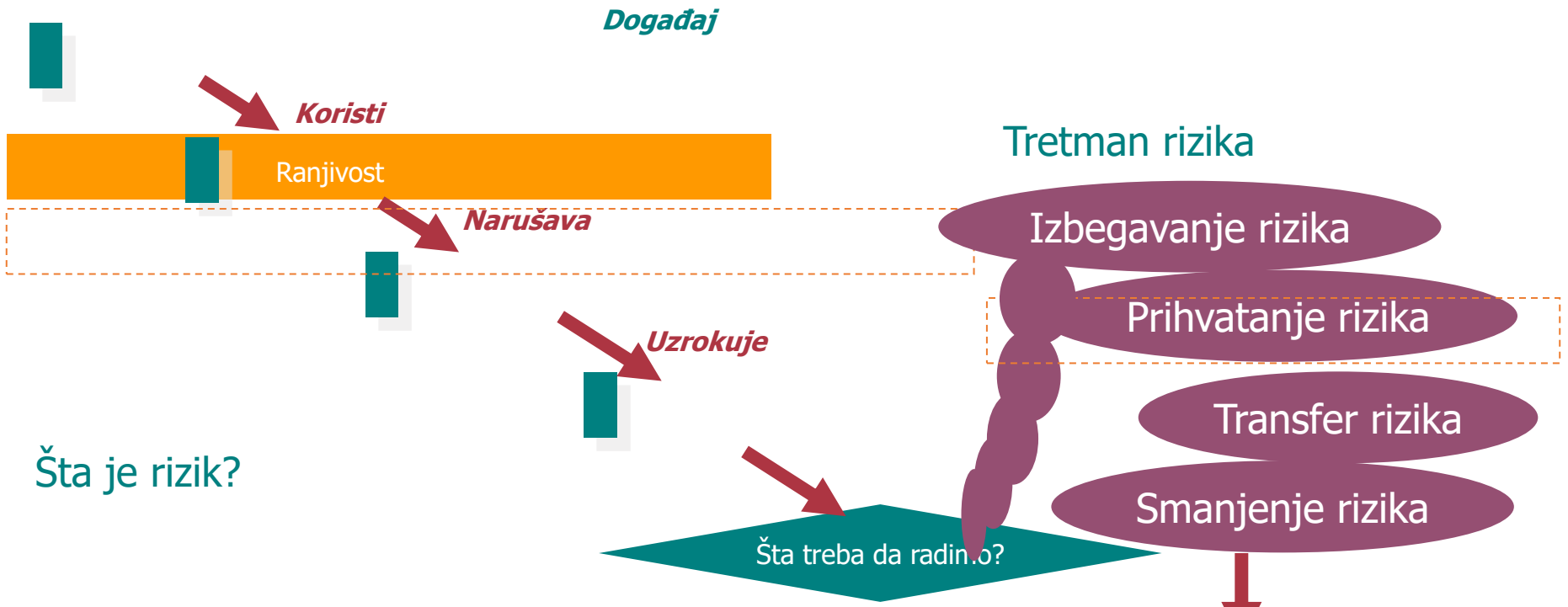
Istorijat serije standarda ISO 27001

Važni datumi

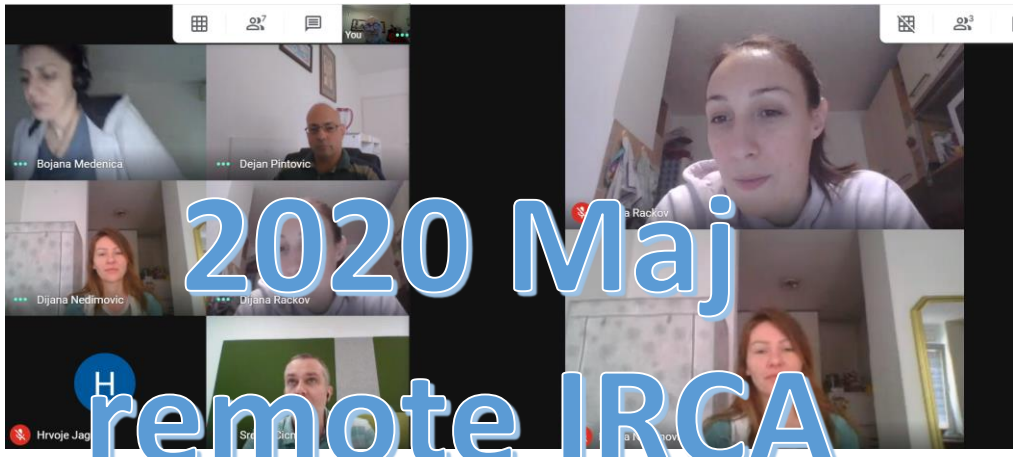
ISO/IEC 27001
tačke standarda (Prilog 'A')



Planovi za tretman rizika



- Proporcionalnost → kontrole treba da odgovaraju riziku
- Odlučiti koje od 114 kontrole date u aneksu A su primenljive



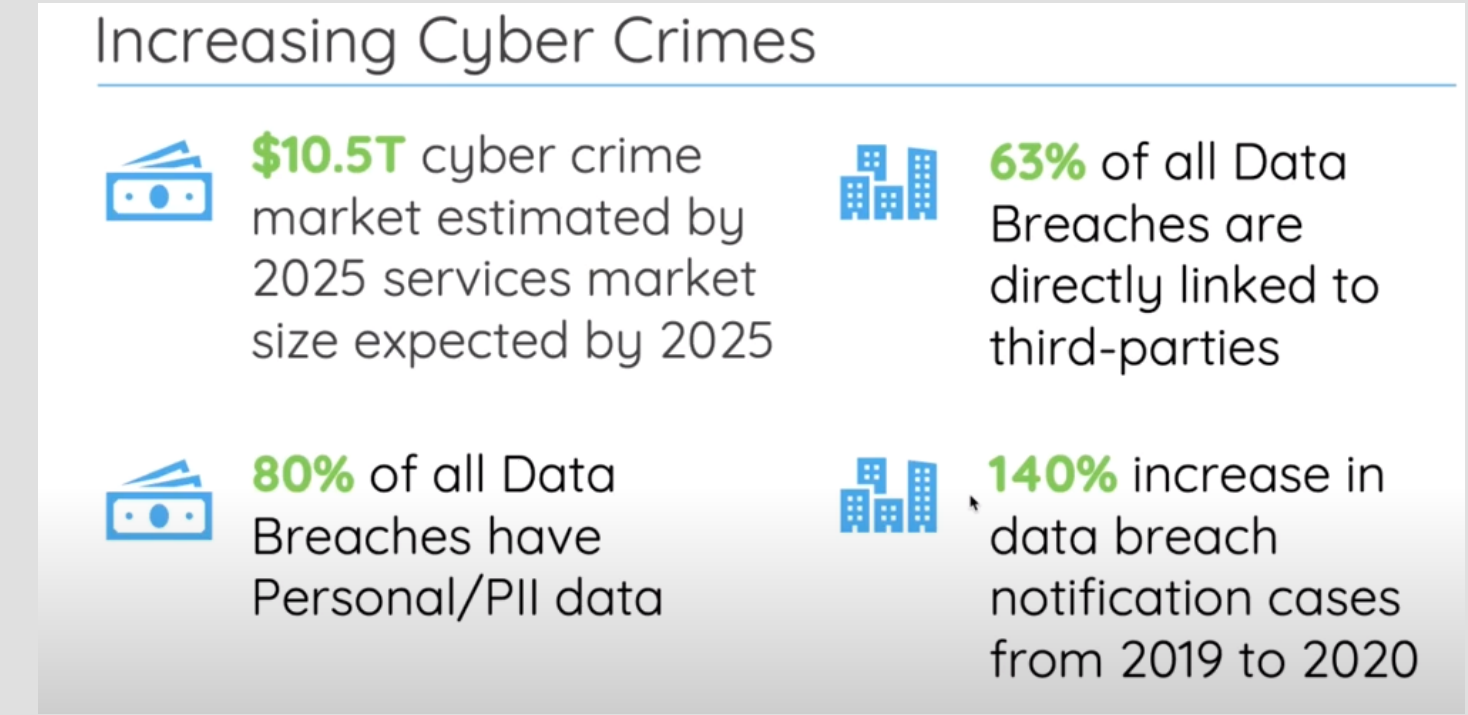
A kod nas

- SRPS ISO/IEC 27001:2014
- Cor 1:2014 and Cor 2:2015

- SRPS ISO/IEC 27002:2015

GODINA	BROJ SERTIFIKTA	BROJ LOKACIJA
2019	258	380
2020	351	499

I dalje kretanja na globalnom tržištu mnogo brze idu nego primena standarda



A tek problemi sa bezbednosti

Some Hefty Privacy / Data Breach Fines

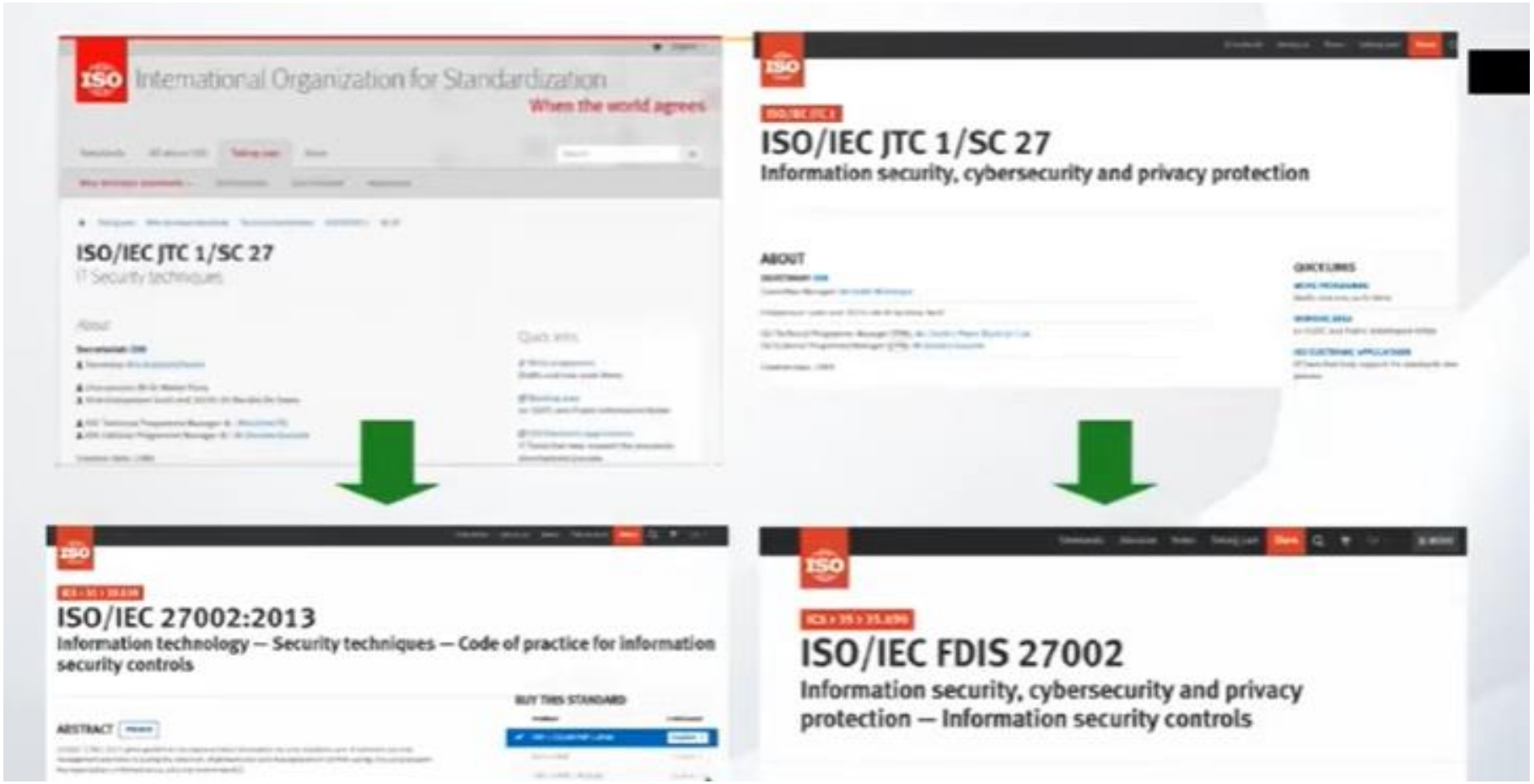
Name	Amount in USD
Facebook	5 billion
Equifax	575 million
British Airways	230 million
Uber	148 million
Marriott	123 million
Yahoo	85 million
Google	50 million
Tesco bank	21 million
Anthem	16 million

Novosti sa standardima “ISO27k”

Zašto ih malo koristimo i poznajemo?

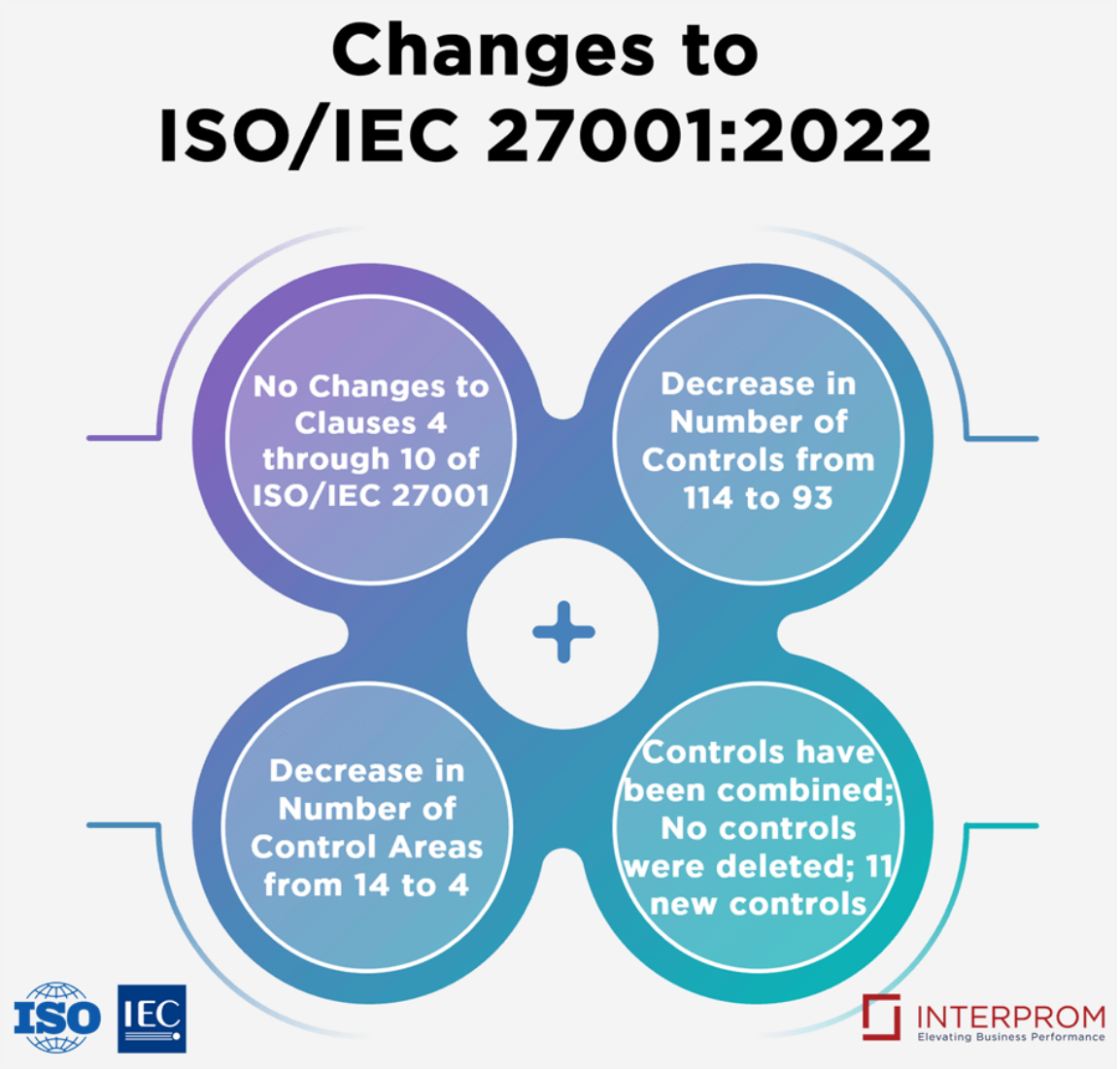
Ukupno 69 standarda

Ko je u ISO ovo radio?



IZMENE ISO 27001&27002

- ISO 27002 je ažuriran 15. februara 2022. godine, a Aneks A od ISO 27001 biće usklađen sa tim promenama.
- Ispravke u ISO 27001 Aneks A će se desiti negde tokom 2022, datum još nije saopšten.
- Tranzicija još nije utvrđena.



Šta je sa ISO 27001?

- Dok će glavne klauzule sistema menadžmenta standarda ISO 27001 ostati iste, Aneks A standarda će biti izmenjen tako da uključuje novi kontrolni set ISO 27002:2022 i očekuje se da će ažurirana verzija biti objavljena u Q3 od 2022.U pripremi je ustvari izmena samo Aneksa A i vodi se diskusija u ISO, u postupku je usvajanja.
- Važno je napomenuti da dok se ne usvoji nova verzija ISO 27001, vaša Izjava o aplikabilnosti (SOA) i dalje mora da se odnosi na Aneks A od ISO 27001:2013, mada bi bilo dobro da razmotrite najnoviji i najsavremeniji set kontrola.

Glavne promene u ISO 27001:2022:

- Glavni deo ISO 27001, ili,klauzule od 4 do 10, se ne menjaju
- Ažuriraće se samo bezbednosne kontrole navedene u ANEKSU ISO 27001 A
- Broj kontrola se smanjio sa 114 na 93
- Kontrole su postavljene u 4 odeljka umesto u prethodnih 14
- Postoji 11 novih kontrola,a mnoge kontrole su objedinjene

Kratka analiza

Predmet	ISO 27002:2022	ISO 27002:2013
Godina od poslednjeg izdanja	9	8
Strana	152	80
Normativne reference	0	1
Termini definicije	38	0
Skraćenice	45	0
Klauzule	4	14
Kontrole	93	114

I SAM NASLOV UKAZUJE

Novi naslov

„Information security, cybersecurity and privacy protection — Information security controls"

„Information technology — Security techniques — Code of practice for information security controls"

Srodni međunarodni standardi

Preporuke za primenu

- Iako ovaj dokument nudi smernice o širokom spektru kontrola informacione bezbednosti koje se obično primenjuju u mnogim različitim organizacijama, drugi dokumenti u porodici ISO/IEC 27000 pružaju komplementarne savete ili zahteve o drugim aspektima ukupnog procesa upravljanja informacionom bezbednošću.
- Pogledajte ISO/IEC 27000 za opšti uvod i za ISMS i za porodicu dokumenata.
- ISO/IEC 27000 obezbeđuje rečnik, definišući većinu termina koji se koriste u celoj ISO/IEC 27000 porodici dokumenata i opisuje opseg i ciljeve za svakog člana porodice.
- Postoje standardi specifični za sektor koji imaju dodatne kontrole koje imaju za cilj rešavanje specifičnih oblasti (npr.ISO/IEC 27017 za usluge u oblaku, ISO/IEC 27701 za privatnost, ISO/IEC 27019 za energetiku, ISO/IEC 27011 za telekomunikacione organizacije i ISO 27799 za zdravlje). Takvi standardi su uključeni u Bibliografiju, a neki od njih se upućuju na smernice i druge odeljke sa informacijama u odredbama 5-8.

Terms, definitions and abbreviated terms

Asset – imovina-sredstva

sve što ima vrednost za organizaciju

Napomena 1 : U kontekstu informacione bezbednosti mogu se razlikovati dve vrste inovine-sredstava:

- **primarna sredstva**:
  - informacija;
  - poslovnih procesa i aktivnosti;
- **sredstva za podršku** (na koju se oslanjaju primarna sredstva) svih tipova, na primer:
  - Hardver;
  - Softver;
  - Mrežne;
  - Osoblje
  - Lokacije
  - Struktura organizacije.

Terms, definitions and abbreviated terms

poverljive informacije

informacije koje nisu namenjene da budu dostupne ili obelodanjene neovlašćenim licima, entitetima ili procesima

Terms, definitions and abbreviated terms

topic-specific policy

intentions and direction on a specific subject or topic, as formally expressed by the appropriate level of management

Note 1 to entry: Topic-specific policies can formally express *rules* (3.1.32) or organization standards.

Note 2 to entry: Some organizations use other terms for these topic-specific policies.

Note 3 to entry: The topic-specific policies referred to in this document are related to information security.

EXAMPLE Topic-specific policy on *access control* (3.1.1), topic-specific policy on clear desk and clear screen.

Terms, definitions and abbreviated terms

- **Napad (attack)**
- uspešan ili neuspešan neovlašćeni pokušaj uništavanja, izmene, onemogućavanja, pristupa imovini ili bilo kakav pokušaj razotkrivanja, krađe ili neovlašćenog korišćenja imovine.

Terms, definitions and abbreviated terms

ABAC attribute-based access control

ACL access control list

IAM identity and access management

IDE integrated development environment

IDS intrusion detection system

IoT internet of things

IPS intrusion prevention system

MAC mandatory access control

PIA privacy impact assessment

RBAC role-based access control

RPO recovery point objective

RTO recovery time objective

SDN software-defined networking

SIEM security information and event management

SMS short message service

SQL structured query language

SSO single sign on

SWID software identification

UEBA user and entity behaviour analytics

VM virtual machine

PII personally identifiable information

Zahtevi za informacionu bezbednost - da se podsetimo?

- Od suštinskog je značaja da organizacija utvrdi svoje zahteve za informacionu bezbednost.
- Postoje tri glavna izvora zahteva za informacionu bezbednost:
- a) procenu rizika po organizaciju, uzimajući u obzir ukupnu poslovnu strategiju i ciljeve organizacije. To se može olakšati ili podržati putem procene rizika specifične za informacionu bezbednost. To bi trebalo da rezultira utvrđivanjem kontrola neophodnih da bi se osiguralo da rezidualni rizik za organizaciju zadovoljava kriterijume prihvatanja rizika;
- b) zakonske, statutarne, regulatorne i ugovorne zahteve koje organizacija i njene zainteresovane strane (trgovinski partneri, pružaoci usluga itd.) moraju da ispoštuju i svoje sociokulturno okruženje;
- c) skup principa, ciljeva i poslovnih zahteva za sve korake životnog ciklusa informacija koje je organizacija razvila da podrži njeno poslovanje.

4 Struktura ovog dokumenta

- **4.1 Klauzule**
- Ovaj dokument je strukturiran na sledeći način:
- a) Organizacione kontrole (Klauzula 5)
- b) Kontrole ljudi (Klauzula 6)
- c) Fizičke kontrole (Klauzula 7)
- d) Tehnološke kontrole (Klauzula 8)
- **4.2 Teme i atributi**
- **4.3 Raspored layout kontrola**
- **5 – 8 Kontrole**
- Postoje 2 informativna aneksa:
- — Annex A — Korišćenje atributa
- — Annex B — Upoređnje sa ISO/IEC 27002:2013
- Aneks A objašnjava kako organizacija može da koristi atribute (pogledajte 4.2) da bi kreirala sopstvene prikaze na osnovu kontrolnih atributa definisanih u ovom dokumentu ili sopstvenom kreiranju.
- Aneks B prikazuje upoređenje između kontrola u ovom izdanju ISO/IEC 27002 i prethodnog izdanja iz 2013.

4 Struktura ovog dokumenta

- **4.3 Raspored layout kontrola**
- Raspored za svaku kontrolu sadrži sledeće:
- **— Naslov kontrole: Kratko ime kontrole**;
- **— Tabela atributa: Tabela prikazuje vrednosti svakog atributa za datu kontrolu**;
- **— Kontrola:** Šta je kontrola;
- **— Svrha:** Zašto kontrola treba da se sprovede;
- **— Smernice :** Kako kontrola treba da se sprovede;
- **— Ostale informacije:** Objašnjenje teksta ili referenci na druge srodne dokumente.
- Podnasloni se koriste u tekstu navođenja za neke kontrole da bi se pomogla čitljivost gde je smernica dugačka i koja se odnosi na više tema. Takvi naslovi se ne koriste nužno u svim tekstovima smernica.
- Podnaslovi su podvučeni.

Tako da zahtev – klauzula izgleda ovako na primer!

5.5 Contact with authorities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Control

The organization should establish and maintain contact with relevant authorities.

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

Guidance

The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

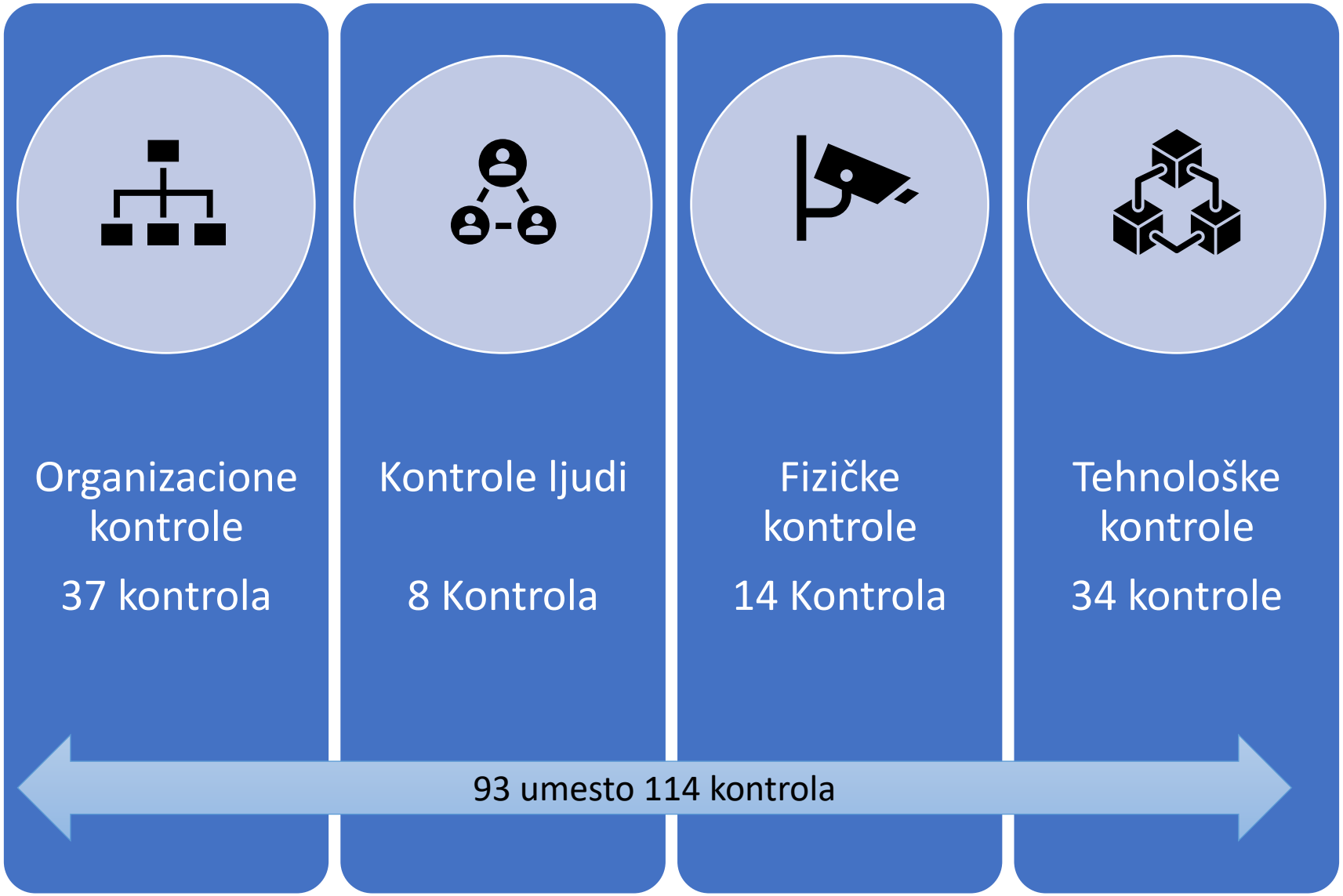
Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

Other information

Organizations under attack can request authorities to take action against the attack source.

Maintaining such contacts can be a requirement to support information security incident management (see 5.24 to 5.28) or the contingency planning and business continuity processes (see 5.29 and 5.30). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety [e.g. fire departments (in

Koliko kontrola ima?



Znači kontrole -93

57
Kontrola

Spojene

24
Kontrole

35 Kontrole ostaju iste
23 Preimenovane kontrole
11 Nove kontrole

Aneks A je izmenjen na sledeći način:

a) Organizational controls (Clause 5)

b) People controls (Clause 6)

c) Physical controls (Clause 7)

d) Technological controls (Clause 8)

11 novih kontrola uvedenih u reviziji ISO 27001 2022:

Biće ažurirane samo bezbednosne kontrole navedene u Aneksu A ISO 27001 i ISO 27002.

- A.5.7 Threat intelligence
- A.5.23 Information security for use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding

Prva novina

New Controls (11)

Type of control	Control
Organizational control	5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulner- ability_management	#Defence #Resilience

Control:
Information relating to information security threats should be collected and analysed to produce threat intelligence.

Guidance:
Information about existing or emerging threats is collected and analysed in order to:
a) facilitate informed actions to prevent the threats from causing harm to the organization;
b) reduce the impact of such threats.
Threat intelligence can be divided into three layers, which should all be considered:
a) strategic threat intelligence: exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks);
b) tactical threat intelligence: information about attacker methodologies, tools and technologies involved;
c) operational threat intelligence: details about specific attacks, including technical indicators. .....

Druga

New Controls (11)

Type of control	Control
Organizational control	5.23 Information security for use of cloud services

Control:
Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Guidance:
The organization should define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how an organization manages services provided by external parties (see 5.21 and 5.22).

The use of cloud services can involve shared responsibility for information security and collaborative effort between the cloud service provider and the organization acting as the cloud service customer. It is essential that the responsibilities for both the cloud service provider and the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately. .....

Treća

New Controls (11)

Type of control	Control
Organizational control	5.30 ICT readiness for business continuity

Control:
ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Guidance:
ICT readiness for business continuity is an important component in business continuity management and information security management to ensure that the organization's objectives can continue to be met during disruption.

The ICT continuity requirements are the outcome of the business impact analysis (BIA). The BIA process should use impact types and criteria to assess the impacts over time resulting from the disruption of business activities that deliver products and services. The magnitude and duration of the resulting impact should be used to identify prioritized activities which should be assigned a recovery time objective (RTO). The BIA should then determine which resources are needed to support prioritized activities .....

Četvrta

New Controls (11)

Type of control	Control
Physical control	7.4 Physical security monitoring

Control:
Premises should be continuously monitored for unauthorised physical access.

Guidance:
Physical premises should be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical
security information management software either managed internally or by a monitoring service provider.

Access to buildings that house critical systems should be continuously monitored.....

Peta

New Controls (11)

Type of control	Control
Technological control	8.9 Configuration management

Control:
Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Guidance:
The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.

Roles, responsibilities and procedures should be in place to ensure satisfactory control of all configuration changes.....

Šesta

New Controls (11)

Type of control	Control
Technological control	8.10 Information deletion

Control:
Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Guidance:
Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.

When deleting information on systems, applications and services, the following should be considered:
a) selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations;
b) recording the results of deletion as evidence;
c) when using service suppliers of information deletion, obtaining evidence of information deletion from them. .....

Sedma

New Controls (11)

Type of control	Control
Technological control	8.11 Data masking

Control:
Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Guidance:
Where the protection of sensitive data (e.g. PII) is a concern, the organization should consider hiding such data by using techniques such as **data masking, pseudonymization or anonymization**.

Pseudonymization or anonymization techniques can hide PII, disguise the true identity of PII principals or other sensitive information, and disconnect the link between PII and the identity of the PII principal or the link between other sensitive information.

When using pseudonymization or anonymization techniques, it should be verified that data has been adequately pseudonymized or anonymized. Data anonymization should consider all the elements of the sensitive information to be effective. As an example, if not considered properly, a person can be identified even if the data that can directly identify that person.....

Osma

New Controls (11)

Type of control	Control
Technological control	8.12 Data leakage prevention

Control:
Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Guidance:
a) identifying and classifying information to protect against leakage (e.g. personal information, pricing models and product designs);
b) monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);
c) acting to prevent information from leaking (e.g. quarantine emails containing sensitive information). .....

Deveta

New Controls (11)

Type of control	Control
Technological control	8.16 Monitoring activities

Control:
Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Guidance:
The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods.

The following should be considered for inclusion within the monitoring system:
a) outbound and inbound network, system and application traffic;
b) access to systems, servers, networking equipment, monitoring system, critical applications, etc.;
c) critical or admin level system and network configuration files;
d) logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention];
e) event logs relating to system and network activity .....

Deseta

New Controls (11)

Type of control	Control
Technological control	8.23 Web filtering

Control:
Access to external websites should be managed to reduce exposure to malicious content.

Guidance:
The organization should identify the types of websites to which personnel should or should not have access. The organization should consider blocking access to the following types of websites:
a) websites that have an information upload function unless permitted for valid business reasons;
b) known or suspected malicious websites (e.g. those distributing malware or phishing contents);
c) command and control servers;
d) malicious website acquired from threat intelligence
e) websites sharing illegal content .....

Jedanesta

New Controls (11)

Type of control	Control
Technological control	8.28 Secure coding

Control:
Secure coding principles should be applied to software development.

Guidance:
The organization should establish organization-wide processes to provide good governance for secure coding. A minimum secure baseline should be established and applied. Additionally, such processes and governance should be extended to cover software components from third parties and open-source software.

The organization should monitor real world threats and up-to-date advice and information on software vulnerabilities to guide the organization's secure coding principles through continual improvement and learning. This can help with ensuring effective secure coding practices are implemented to combat the fast-changing threat landscape. .....

IZBRISANE KONTROLE (16)

Kada se bude preuređivao SoA obratiti pažnju na ove elemente ISMS

1. Review of the policies for security
2. Ownership of assets
3. Password management system
4. Restrictions on software installation
5. Protection of log information
6. Securing application services public networks
7. Protecting application services transactions
8. Reporting information security weaknesses

9. Mobile device policy
10. Handling of assets
11. Delivery and loading areas
12. Unattended user equipment
13. Removal of assets
14. Electronic messaging
15. System acceptance testing
16. Technical compliance review

Promena naziva kontrole -23

Stare kontrole iz ISO 27002:2013	Kontrole u novom ISO 27002:2022
6.2.2 Teleworking	6.7 Remote working
7.3.1 Termination or change of employment responsibilities	6.5 Responsibilities after termination change Of reemployment
9.2.1 User registration and de-registration	5.16 identity management
9. 2.3 Management of privileged access rights	8.2 Privileged access rights
9.4.2 Secure log-on procedures	8.5 Secure authentication
9.4.5 Access control to program source code	8.4 Access to source code
11.1.1 Physical security perimeter	7.1 Physical security perimeters
11.2.6 Security of equipment and assets off-premises	7.9 Security Of assets off-premises
11.2.9 Desk and clear screen policy	7.7 Clear desk and clear screen
12.2.1 Controls against malware	8.7 Protection against malware

Promena naziva kontrole -23

Stare kontrole iz ISO 27002:2013	Kontrole u novom ISO 27002:2022
12.7.1 Information systems audit control	8.34 Protection of information systems during audit testing
13.1.1 Network controls	8.20 Networks security
13.13 Segregation in networks	8.22 Segregation of networks
14.21 Secure development policy	8.25 Secure development life cycle
14.2.S Secure system engineering principles	8.27 Secure system architecture and engineering principles
14.3.1 Protection of test data	8.33 Test information
15.1.1 Information security policy for supplier relationships	5.19 Security in supplier relationships
15.1.2 Addressing security within supplier agreements	5.20 Addressing information security within supplier agreement
15.1.3 Information and communication technology supply	5.21 Managing information security in the ICT supply chain

Promena naziva kontrole -23

Stare kontrole iz ISO 27002:2013	Kontrole u novom ISO 27002:2022
16.1.1 Responsibilities and procedures 16.1.4 Assessment of and decision on information 17.2.1 Availability of information processing facility 18.1.4 Privacy and protection of personally identifiable	5.24 Information security incident management planning and preparation 5.25 and decision on information security events security events 8.14 Redundancy of information processing facilities 5.34 5.34 Privacy and protection of PII

MERGED CONTROLS

A. 5 Original Controls	Merged controls in 27002:2022
5.1.1 Policies for information security 5. I .2 Review Of the policies information security	5.1 Policies for information security
A.6 and A.14 Original Controls	
6.1.5 Information security in project management 14.1.1 Information security requirements analysis and specification	5.8 Information Security in Project
A.6 and A.11 Original Controls	
6.2.1 Mobile device 1 1.2.8 Unattended user equipment	8.1 User End Device
A.8 Original Controls	
A.8.1.1Inventory of assests A.8.1.2 Ownership of assets	5.9 Inventory of information and other associated assets

MERGED CONTROLS

A.9 Original Controls	Merged controls in 27002:2022
9.2.4 Management of secret authentication information of users 9.3.1 use of secret authentication information 9.4.3 Password management system	5.17 Authentification information
A.10 Original Controls	
10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management	8.24 Use of cryptography
A. 11 Original Controls	
A 11.1.2 Physical entry control A 11.1.6 Delivery and Loading areas	7.2 Physical entry

MERGED CONTROLS

A. 12 and A. 14 Original Controls	Merged controls in 27002:2022
12.1.2 Change management 14.2.2 System change control procedures 14.2.3 Technical review of applications after operating platform changes 14.2.4 Restrictions on changes to software packages	8.32 Change management
12.1.4 Separation of development, testing, and operational environments 14.2.6 Secure development environment	8.31 Separation of development. test and production environments
A. 12 and A.18 Original Controls	
12.4.1 Event logging 12.4.2 Protection of log information 12.4.3 Administrator and operator logs	8.15 Logging

MERGED CONTROLS

A.14 Original Controls	Merged controls in 27002:2022
14.1.2 Securing application services public networks 14.1.3 Protecting application services transactions	8.26 Application security requirements
14.2.8 System security testing 14.2.9 System acceptance testing	8.29 Security testing in development and acceptance
A.15 Original Controls	
15.2.1 Monitoring and review of supplier services 15.2.2 Managing changes to supplier services	5.22 Monitoring, review, and change management of supplier services
A.16 Original Controls	
16.1.2 Reporting information security event 16.1.3 Reporting information Security weaknesses	6.8 Information security events reporting

MERGED CONTROLS

A 17 Original Controls	Merged controls in 27002:2022
17.1.1 Planning information security continuity 17.1.2 Implementing information security continuity 17.1.3 Verify, review and evaluate information security continuity	5.29 Information security during disruption
A.18 1 Original Controls	
18.1.1 Identification of applicable legislation and contractual requirements 18.1.5 Regulation of cryptographic controls	5.31 Legal. statutory. regulatory and contractual requirements
18. 2.2 Compliance with security policies and standards 18.23 Technical compliance review	5.36 Conformance with policies, rules and standards for information security

Nove kontrole:

Control	Type of control
5.7 Threat intelligence	Organizational
5.23 Information security for use of cloud services	Organizational
5.30 ICT readiness for business continuity	Organizational
7.4 Physical security monitoring	Physical
8.9 Configuration management	Technological
8.10 Information deletion	Technological
8.11 Data masking	Technological
8.12 Data leakage prevention	Technological
8.16 Monitoring activities	Technological
8.23 Web filtering	Technological
8.28 Secure coding	Technological

Teme:

Kontrole su sada grupisane u 4 "teme", a ne u prethodnih 14 skupova, u zajedničkim kategorijama, ove su:

Organizacione (37 Kontrole)

Tehnološke (34 Kontrole)

Fizičke (14 controls)

Kontrole Ljudi (8 Kontrole)

Kao primer kontrolne strukture u ISO/IEC 27002:2022 možete videti tabelu atributa:

Tip kontrole	Svojstva informacione bezbednosti	Koncepti sajber bezbednosti	Operativne mogućnosti	Bezbednosni domeni
#Preventine #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

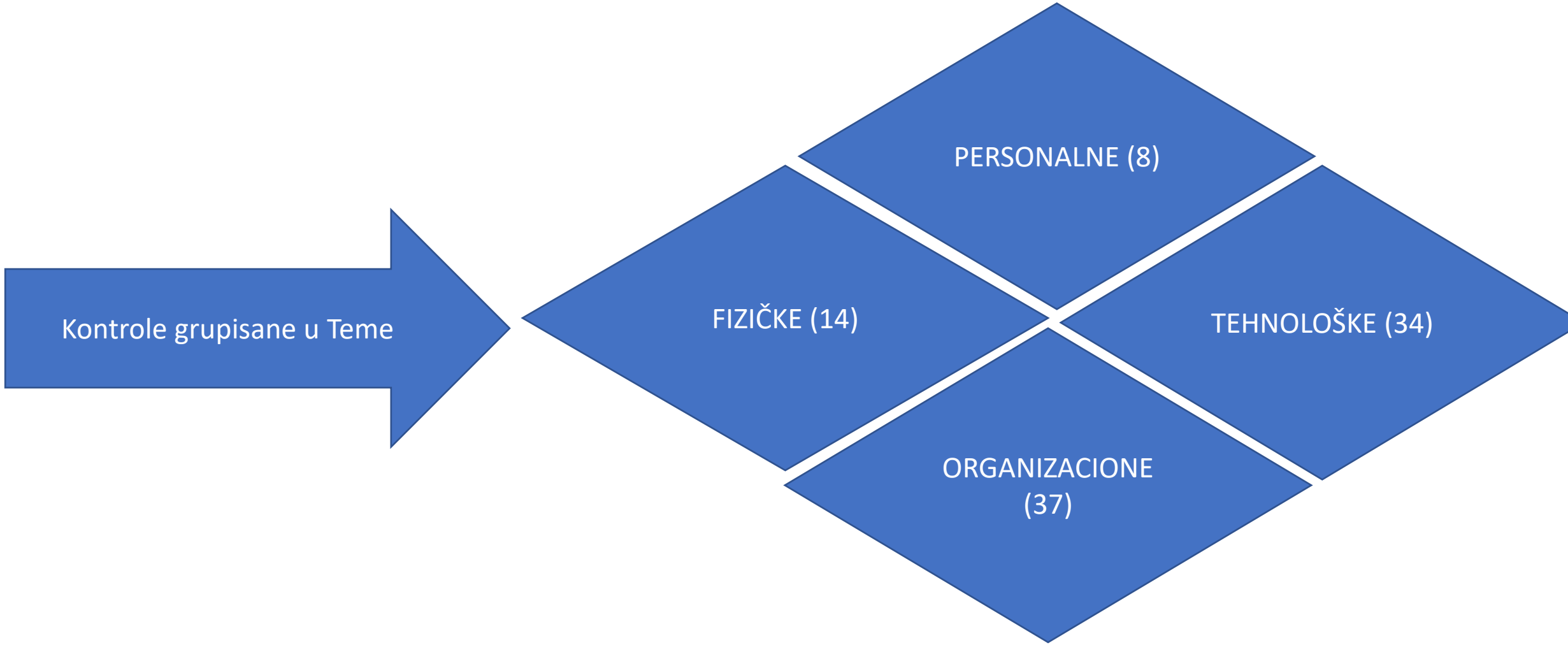
5.6 Kontakt sa posebnim interesnim grupama:

Kontrola
Organizacija treba da uspostavi i održi kontakt sa posebnim interesnim grupama ili drugim specijalističkim bezbednosnim forumima i strukovnim udruženjima
Svrha:
Da bi se obezbedio odgovarajući protok informacija, odvija se u odnosu na informacionu bezbednost.
Uputstvo
Članstvo posebnih interesnih grupa ili foruma treba uzeti u obzir kao sredstvo za:
a) usavršava znanje o najboljim praksama i bude u toku sa relevantnim bezbednosnim informacijama;
b) obezbediti da je razumevanje okruženja za informacionu bezbednost aktuelno;
c) dobija ranih sašnanja o upozorenjima, savetima i zakrpama koje se odnose na napade i ranjivosti;
d) dobije pristup specijalističkim savetima za informacionu bezbednost;
e) deli i razmenjuje informacije o novim tehnologijama, proizvodima, uslugama, pretnjama iliranjivosti;
f) obezbediti odgovarajuće mogućnosti za veze, kada se radi o incidentima vezanim za informacionu bezbednost (videti od 5.24 do 5.28).
Ostale informacije
Nema drugih informacija.

Razumevanje novih tema ISO 27002

- Pre nego što uskočimo u atribute, važno je da prvo razumemo promenu u strukturi kontrole koja se postavlja u okviru novog standarda.
- **Prethodno smo svi razumeli 114 kontrola Aneksa A u okviru ISO 27001:2013, ili A.5 – A.18 koje će biti organizovane u kontrolne ciljeve i osnovne kontrolne aktivnosti.**
- **Ali sada su konsolidovane u skup od četiri klauzule – koje se nazivaju "teme". Standard kategorizuje ove teme na sledeći način:**
- Klauzula 5 – Organizacione
- Klauzula 6 – Ljudi
- Klauzula 7 – Fizičke
- Klauzula 8 – Tehnološke
- **Ovde stižu atributi. One omogućavaju organizacijama da prikažu dublje od samo četiri klauzule ili teme kako bi pružile dublji uvid u bezbednost.**

Kontrole se grupišu u Teme



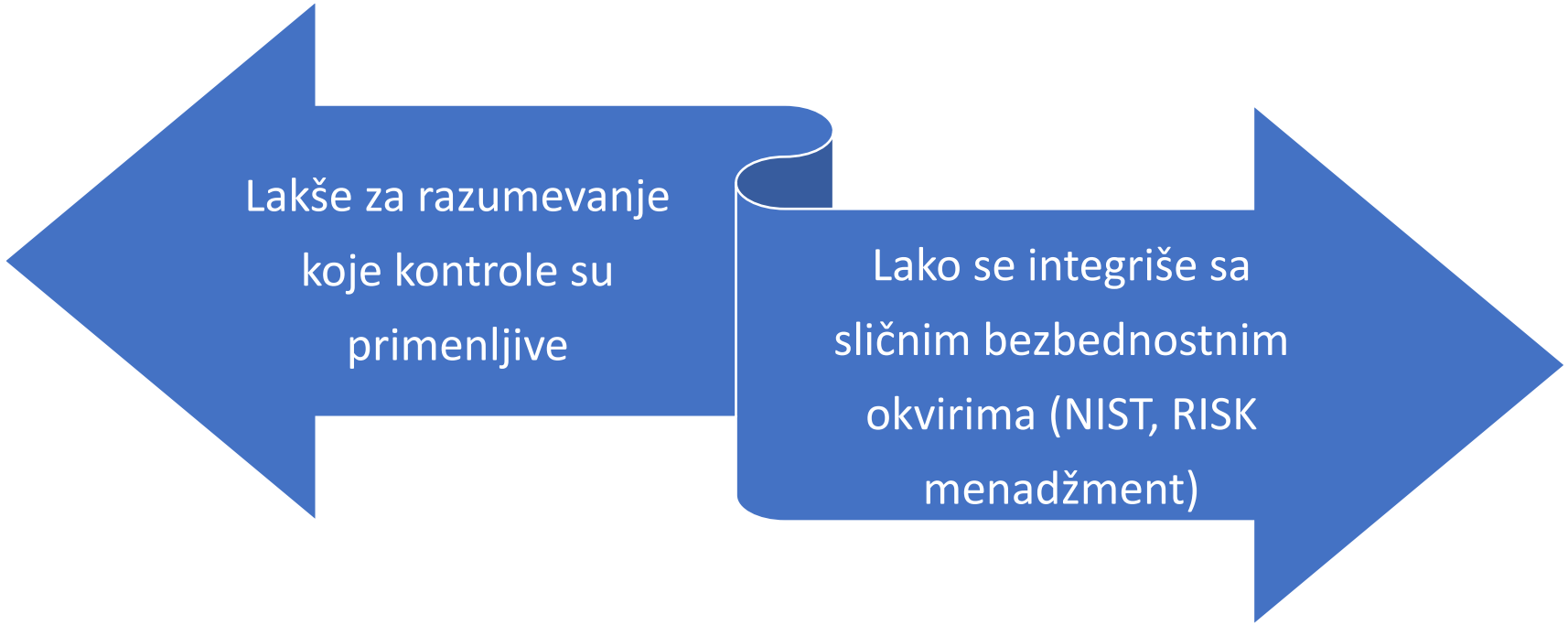
Kada koristiti atribute u ISO 27002

- Ako ne razumemo šta su atribut, možete biti zbunjeni.
- Trebalo bi da ih razmotrite kao alate tokom procesa procene rizika i tretmana/kontrole rizika.
- Oni mogu da ubrzaju ispunjenje ISO 27001 ISMS klauzule 6.1.3 c – što je jedna od njihovih glavnih prednosti.
- Taj zahtev upoređuje kontrole utvrđene procesom tretmana rizika – koje se nazivaju "neophodne" kontrole – sa onima u Aneksu A od ISO 27001 kako biste se uverili da niste prevideli neku od potrebnih kontrola.

Koja je uloga atributa u ISO 27002?

- Ali kako oni zapravo funkcionišu?
- Možda će vam pomoći da o atributima razmišljate kao o pod-kategorijama za kontrole u okviru četiri nove glavne odredbe (5-8) koje smo ranije pomenuli. Te odredbe imaju prilično široke opise – organizacione, osobe, fizičke i tehnološke – ali atributi vam mogu pomoći da odredite više specifičnosti od toga za svaku kontrolu.
- Različiti atributi obezbeđuju različita sočiva za prikazivanje kontrola tako da možete lakše da razaznate da li su vam potrebne ili ne.
- O njima se zapravo detaljno govori u okviru Aneksa A novog standarda ISO 27002, uključujući veoma korisne smernice o tome kako možete da koristite atribute definisane standardom – ili kako da kreirate sopstveni, s obzirom da su oni raznovrsni i prilagodljivi dizajnom.
- Aneks takođe sadrži tabelu koja rezimira vrednosti atributa svake od 93 kontrole u okviru standarda iz 27002.
- Ove jedinstvene perspektive sada nude nove mogućnosti kako biste ubrzali proces izbora i implementacije kontrole i bolje razumeli potencijalne slučajeve korišćenja svake kontrole.

Prednosti kontrolnih atributa



A šta je atribut?

- Atribut je tip karakteristike kontrole
- Vrednost atributa je određena forma ili količina, ili kategorija ili opseg količina za dati atribut.
- Neke vrednosti atributa su diskretne – pojedinačne, posebne, dok druge se mogu prikazivati kao kontinuitet ili spektar.
- U nekim drugim kontekstima, 'atributi' mogu da se odnose na parametre, argumente ili postavke za softverske kontrole (kao što su veličine, boje i radnje koje se pokreću kada korisnici kliknu na dugmad i birače na ekranu) ili na detalje konfiguracije kontrole (kao što su prava i dozvole koje su dodeljene/uskraćene pomoću kontrola pristupa).

O atributima još i ovo

- Obratite pažnju na to da se atributi preklapaju, a nisu alternative. Kontrole se mogu kategorizovati pomoću primenljivih vrednosti atributa iz svih kategorija atributa.

- Pored toga, same vrednosti atributa nisu uvek posebne-pojedinačne, stoga kontrole mogu posedovati više od jedne ili opseg vrednosti za bilo koji atribut, imajući karakteristike nekoliko vrednosti atributa.
- Postoji relacija "više-prema-više" između kontrola informacione bezbednosti, atributa i vrednosti atributa.

Još jedan pogled na Atribute

Table A.1 — Matrix of controls and attribute values

Primer 4 atributi iz samoga standarda

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.37	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

Aneks A ISO 27002:2022

9 stranica ovakve tabele

Table A.1 — Matrix of controls and attribute values

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
5.2	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience
5.3	Segregation of duties	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem
5.4	Management responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

Aneks A ISO 27002:2022

Table A.2 — View of #Corrective controls

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.5	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contact with special interest groups	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Threat intelligence	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
5.24	Information security incident management planning and preparation	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
5.26	Response to information security incidents	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

Primer atributa 1

Atributi & Vrednosti atributa	Kontrole informacione bezbednosti & Aplikacije
Formalnost	
Formalno	Ugovori, zakoni, propisi; smernice; obaveze, zahteve; obavezna kontrola pristupa; provere, inspekcije trećih strana
Neformalno	Sporazumi; smernice, savete, preporuke; standarde; diskrecionu kontrolu pristupa; Preispitivanja

Primer atributa 2

Atributi & Vrednosti atributa	Kontrole informacione bezbednosti & Aplikacije
Snaga-jačina	
Jaka	Biometrijska potvrda identiteta sa svim odgovarajućim kontrolama oko upisa, upravljanja, validacije, „proof-of-life“, itd.
Srednja	Multifaktorna potvrda identiteta pomoću bezbednosnih tokena, komunikacija van opsega itd.
Slaba	Lozinke, fraze za prolaz, PIN kodovi

Primer atributa 3

Atributi & Vrednosti atributa	Kontrole informacione bezbednosti & Aplikacije
Više-multi funkcionalnosti	
Multi-functional	Nadgledanje, supervizija, menadžment i „peer“ preispitivanja
Mono-functional	Dovršavanje kontrolnih lista/tik-liste, pregled logova i tragova provere

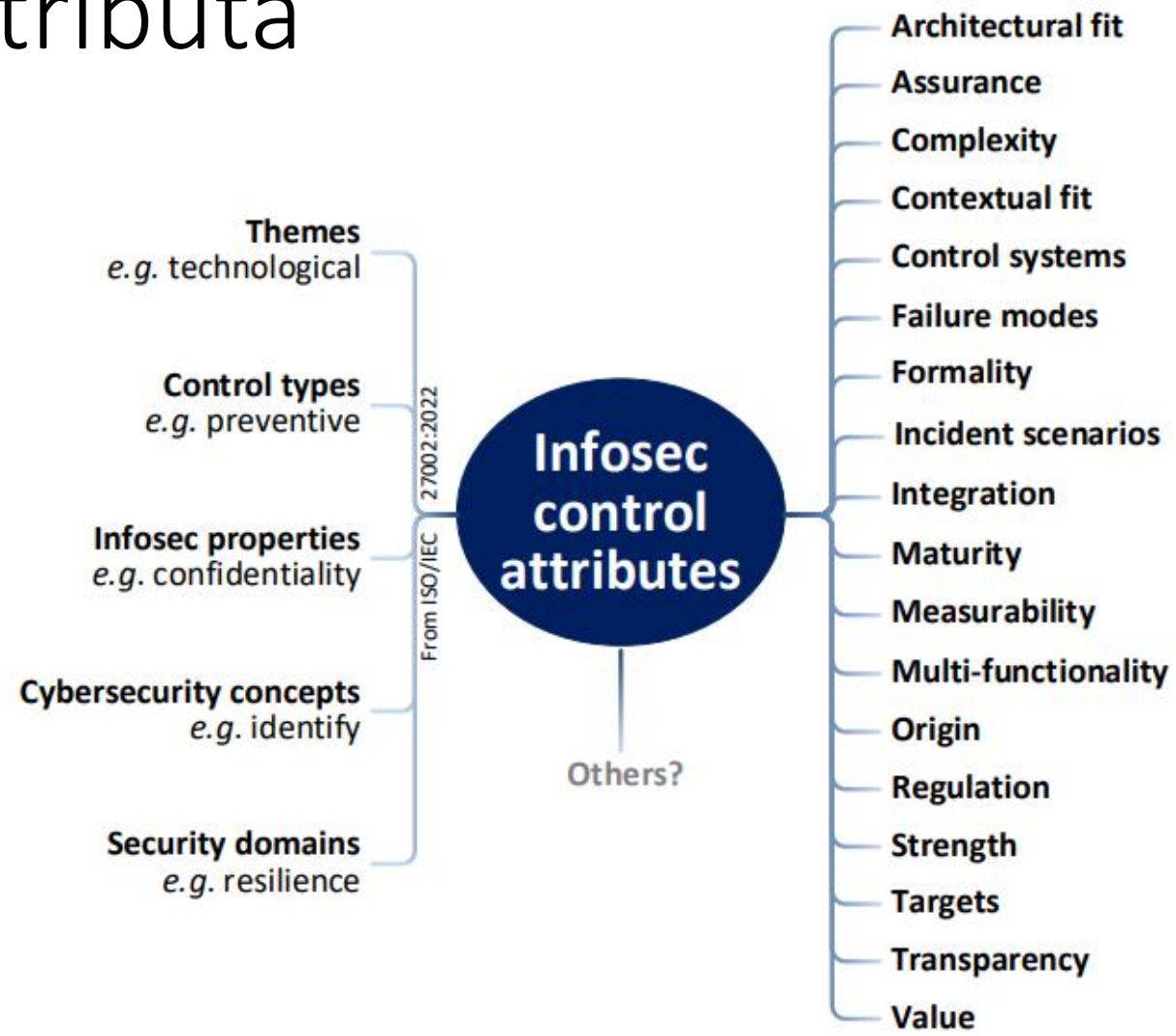
Važno je i ovo

Dodatni kontrolni atributi, pored onih u ISO/IEC 27002 Klauzuli 4.2 ISO/IEC 27002:2022 se mogu koristiti : "Organizacije mogu odabrati da zanemare jedan ili više atributa datih u ovom dokumentu. Oni takođe mogu da kreiraju sopstvene atribute (sa odgovarajućim vrednostima atributa) da bi kreirali sopstvene organizacione prikaze. Klauzula A.2 sadrži primere takvih atributa.”.

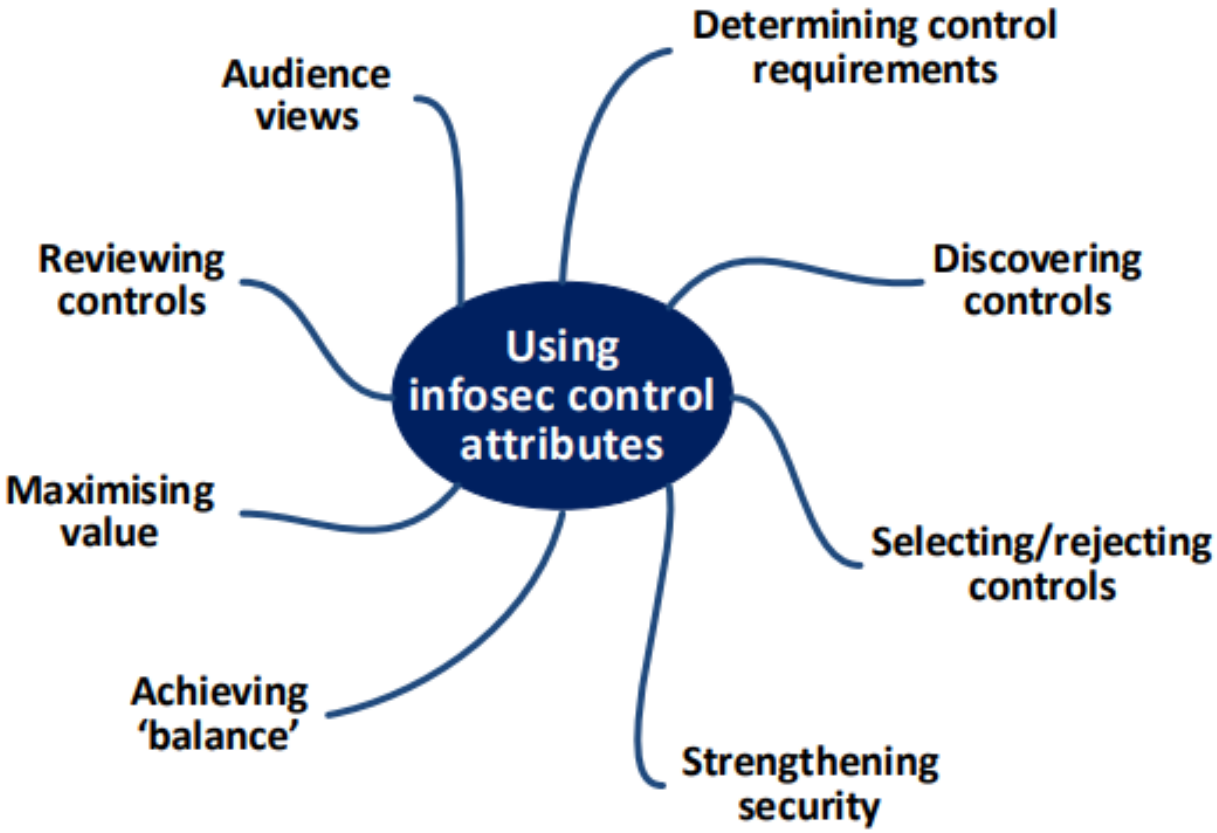
Ovaj odeljak predlaže nekoliko dodatnih atributa koje potencijalno vredi uzeti u obzir, na odgovarajući način.

Kontrolni atributi navedeni u ISO/IEC 27002, kao i drugi opisani u nastavku, primenljivi su u raznim okolnostima. Malo je verovatno da bi organizacija želela da ih koristi odjednom.

Još neki primeri atributa iz literature



Kako se koriste atributi?



ISO/IEC 27028 - Guidelines for ISO/IEC 27002 attributes *[DRAFT]*

ISO/IEC 27028 - Guidelines for ISO/IEC 27002 attributes *[DRAFT]*

Abstract
TBA[Source: none yet] **Introduction**
TBA

Scope of the standard
TBA

Content of the standard

TBA.

Status of the standard

A **P**reliminary **W**ork **I**tem has been approved, and drafting has commenced.

Personal comments

The 2022 3rd edition of ISO/IEC 27002 introduced a new structure for the information security controls, based around 'themes' and 'attributes'. The standard notes that organisations may prefer to use their own attributes as well or instead.

ISO/IEC 27028 *may* explain how to do that, in practice, and *may* suggest a variety of control attributes to classify/characterise information security controls in various ways for various purposes.
Meanwhile, I've written and contributed a white paper to the SC 27 project team to expand the skeletal first draft.

Određivanja kontrola

Utvrđivanje kontrola zavisi od odluka organizacije nakon procene rizika, sa jasno definisanim opsegom.

Odluke vezane za identifikovane rizike treba da budu zasnovane na kriterijumima za prihvatanje rizika, opcijama tretmana rizika i pristupu upravljanju rizicima koji primenjuje organizacija.

Utvrđivanje kontrola takođe bi trebalo da uzme u obzir sve relevantne nacionalne i međunarodne propise.

Utvrđivanje kontrole takođe zavisi od načina na koji kontrole međusobno komuniciraju kako bi se dubinski obezbedila odbrana.

Organizacija može da dizajnira kontrole po potrebi ili da ih identifikuje iz bilo kog izvora.

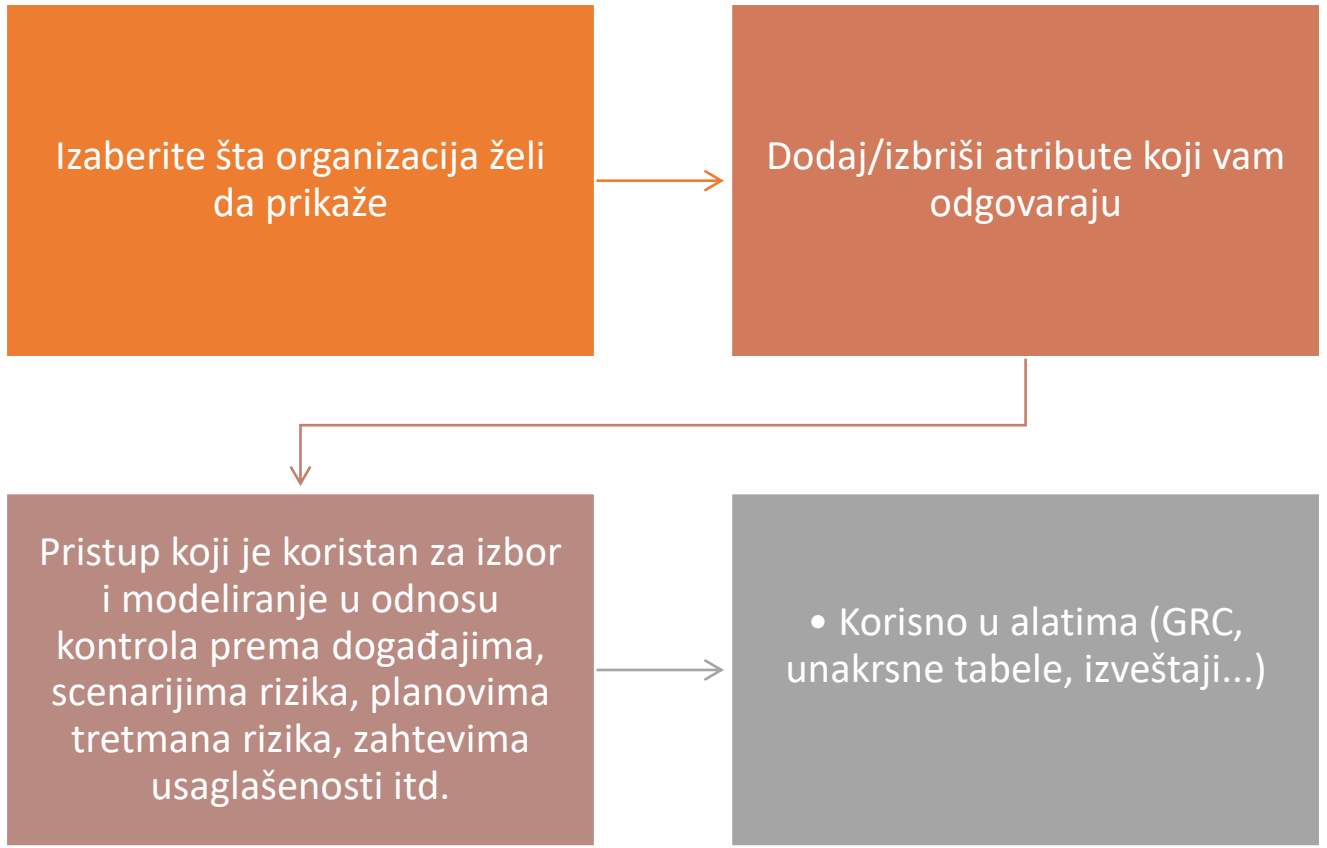
U preciziranju takvih kontrola, organizacija bi trebalo da razmotri resurse i investicije potrebne za sprovođenje i upravljanje kontrolom u odnosu na realizovanu poslovnu vrednost.

Pogledajte ISO/IEC TR 27016 za smernice o odlukama u vezi sa ulaganjem u ISMS i ekonomskim posledicama ovih odluka u kontekstu konkurentskih zahteva za resurse

Kako primeniti (nove) kontrole?

- Pristup zasnovan na riziku — opravdanje isključenja kontrole?
- Zahtevi
- Agilnost
- Jasno definisane uloge i odgovornosti
- Sistem merenja
- Poboljšanja
- Izveštavanje i povratne informacije (troškovi, uticaji)

Upotreba atributa



Koji su sledeći koraci za organizacije koje su već sertifikovane za ISO 27001?

- U smislu sledećih koraka, glavne aktivnosti koje treba da izvršite uključuju sledeće:
- • Kupovina ažuriranog standarda.
  • Pregledajte novi standard ISO 27002 i njegove kontrolne promene.
  • Izvršite procenu/analizu rizika. URM vam može pomoći u ovom procesu.
  • Da biste ublažili sve identifikovane rizike, izaberite kontrole koje su najprimetnije i ažurirajte ISMS smernice, standarde itd..
  • Ažuriranje izjave o odgovornosti (SoA).
- Međutim, ako želite da razumete više o novim kontrolama i šta treba da uradite u smislu pripreme da ih ispoštujete, kontaktirajte nas odmah ili pohađajte naš 1-dnevni kurs obuke za migracije.

Šta ćete morati da uradite?

- Ažuriranje procesa tretmana rizika novim kontrolama
- Ažuriranje izjave o primenljivosti SoA
- Prilagodili određene odeljke u postojećim Politikama i procedurama.

Sledeći koraci

Koristite predstojeće provere da biste procenili status i zahteve novih kontrola za implementaciju

Pripremite se za objavljivanje nove Izjave o primeni (imate 2 ili 3 godine nakon objavljivanja nove verzije ISO 27001)

Uverite se da imate sve dostupne izvore informacija

Počnite ranije sa promenama koje mogu imati značajan uticaj na vaš ISMS

Neke reference koje preporučujem

- ISACA COBIT (originally ‘Control Objectives in Information Technology’).
- ISO/IEC 27001:2013 “Information technology — Security techniques — Information security management systems — Requirements”.
- ISO/IEC 27002:2022 “Information security, cybersecurity and privacy protection — Information security controls”.
- ISO/IEC 27005:2018 “Information technology — Security techniques — Information security risk management”.
- ISO/IEC TS 27008:2019 “Information technology — Security techniques — Guidelines for the assessment of information security controls”.
- ISO/IEC 27028 “Information security, cybersecurity and privacy protection — Guidelines for ISO/IEC 27002 attributes” (currently at the early stages of drafting).
- ISO/IEC TS 27110:2021 “Information security, cybersecurity and privacy protection — Cybersecurity framework development guidelines”.
- **N**ational **I**nstitute of **S**tandards and **T**echnology (2014) “Framework for Improving Critical Infrastructure Cybersecurity” version 1.0.

Dodatak A (informativno) **Korišćenje atributa**

- **A.1 Opšte**
- Ovaj aneks obezbeđuje tabelu koja prikazuje upotrebu atributa kao način kreiranja različitih prikaza kontrola.
- **A.2 Organizacioni prikazi**
- Pošto se atributi koriste za kreiranje različitih prikaza kontrola, organizacije mogu da odbace primere atributa predloženih u ovom dokumentu i kreiraju sopstvene atribute sa različitim vrednostima za rešavanje određenih potreba u organizaciji.

Table A.1 — Matrix of controls and attribute values

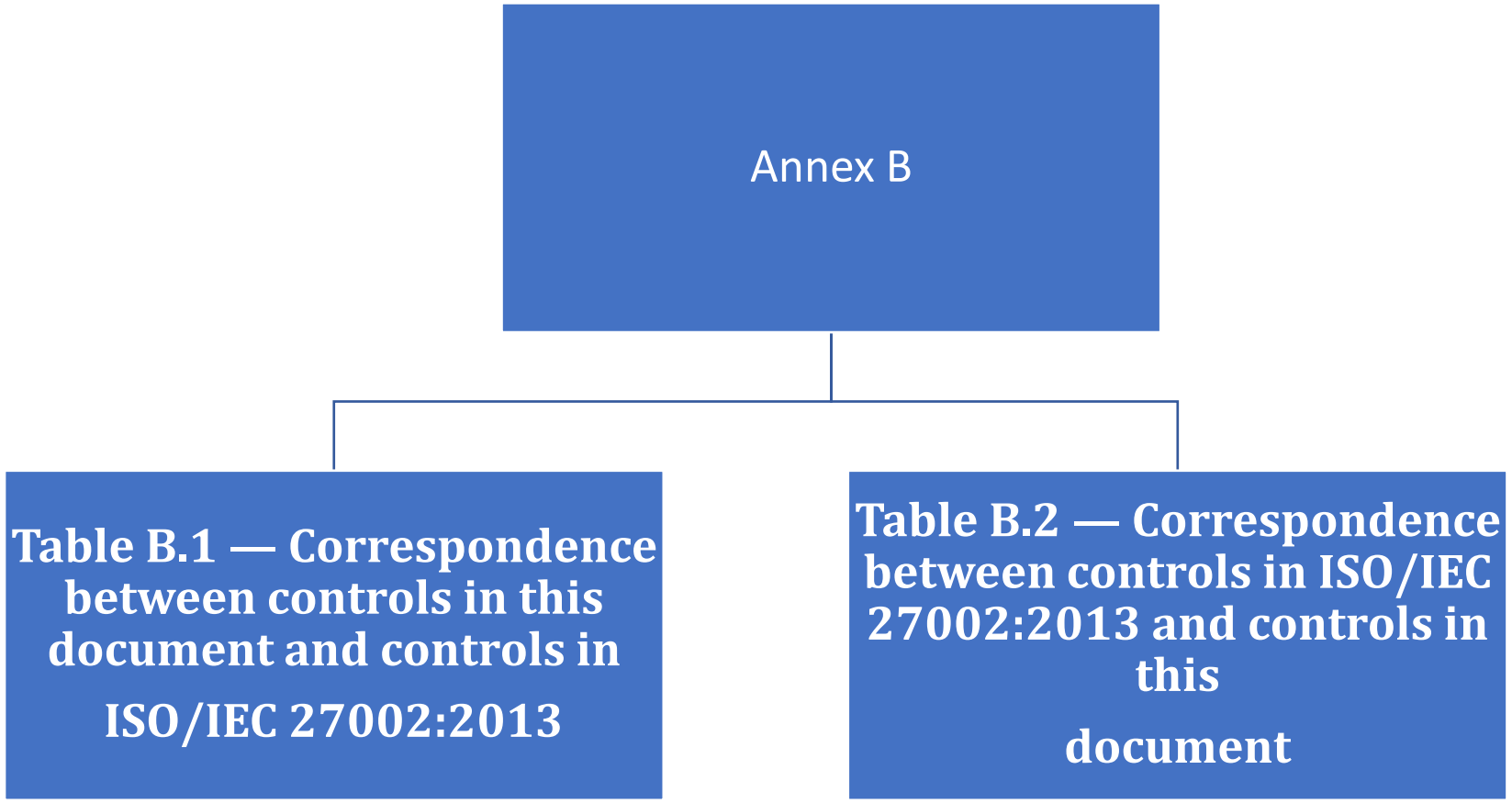
ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
5.2	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience

Table A.2 — View of #Corrective controls

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.5	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contact with special interest groups	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

Dodatak B

- **Dodatak B** (Informativno) **upoređenje ISO/IEC 27002:2022 (ovaj dokument) sa ISO/IEC 27002:2013**



Ovo treba pogledati

NIST CSF – ISO 27002 Cybersecurity concepts attribute – aligned:

https://www.nist.gov/cyberframework

Using attributes

- Select what an organization wants to view
- Add/delete attributes as suitable
- Approach that is useful for navigating the controls' relation to events, risk scenarios, risk treatment plans, compliance requirements, etc.
- Useful in tools (GRC, spreadsheets, reports…)

TEME ZA DISKUSIJU?

KAKO NAM IZGLEDAJU OVE IZMENE U SMISLU PRAKTIČNE PRIMENE I SERTIFIKACIJE?

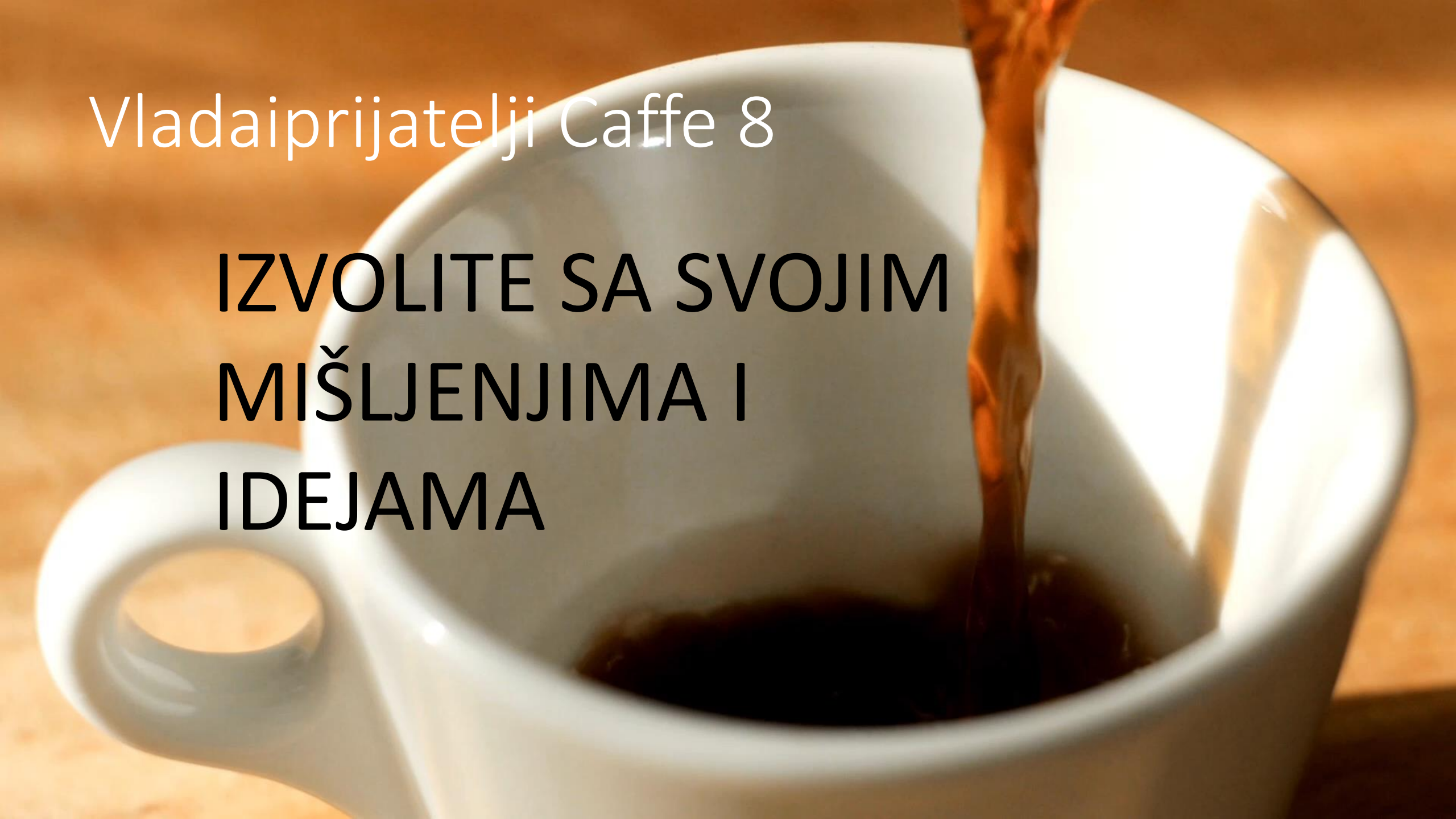
ŠTA SU GLAVNI PROBLEMI U PRIMENI ISO 27001? ZAŠTO SE MALO PRIMENJUJU ?I KAKO IH REŠITI?

ZAŠTO SE STANDARDI IZ SERIJE MALO KORISTE? DA LI SMO SAMI KRIVI ZA TO ILI JE TO POSLEDICA RAZVOJA KORISNIKA STANDARDA I KULTURE STANDARDIZACIJE ?

ŠTA BI BILO DOBRO RADITI?

ŠTA ORGANIZACIJE?

ŠTA OSTALE ZAINTERESOVAANE STRANE?



Vladaiprijatelji Caffe 8

IZVOLITE SA SVOJIM MIŠLJENJIMA I IDEJAMA