

Uvod u usklađenost sa regulativama i standardima iz domena informacione bezbednosti



The better the question. The better the answer.
The better the world works.



Building a better
working world



Виши менаџер,
CISA, ISO27001 LA,
CDPO

EY Serbia



Виши менаџер,
CISSP, CISA, ISO27001 LA,
CDPO

EY Serbia



Области укључене у предмет:

Управљање безбедношћу и ризицима

- Принципи управљања информационом безбедношћу
- Кључни концепти у управљању информационом безбедношћу
- Стратегија информационе безбедности
- Технике стратешког управљања
- Политике и процедуре информационе безбедности
- Управљање ризицима информационе безбедности

Усклађеност са регулативама и стандардима

- Увод у усклађеност са регулативама и стандардима из домена информационе безбедности
- Контролни оквир и окружења у информационој безбедности
- Упознавање са Контролним оквирима најбоље праксе
- Мерење нивоа безбедности (Security Metrics) и извештавање.
- Међународни стандарди и регулативе информационе безбедности

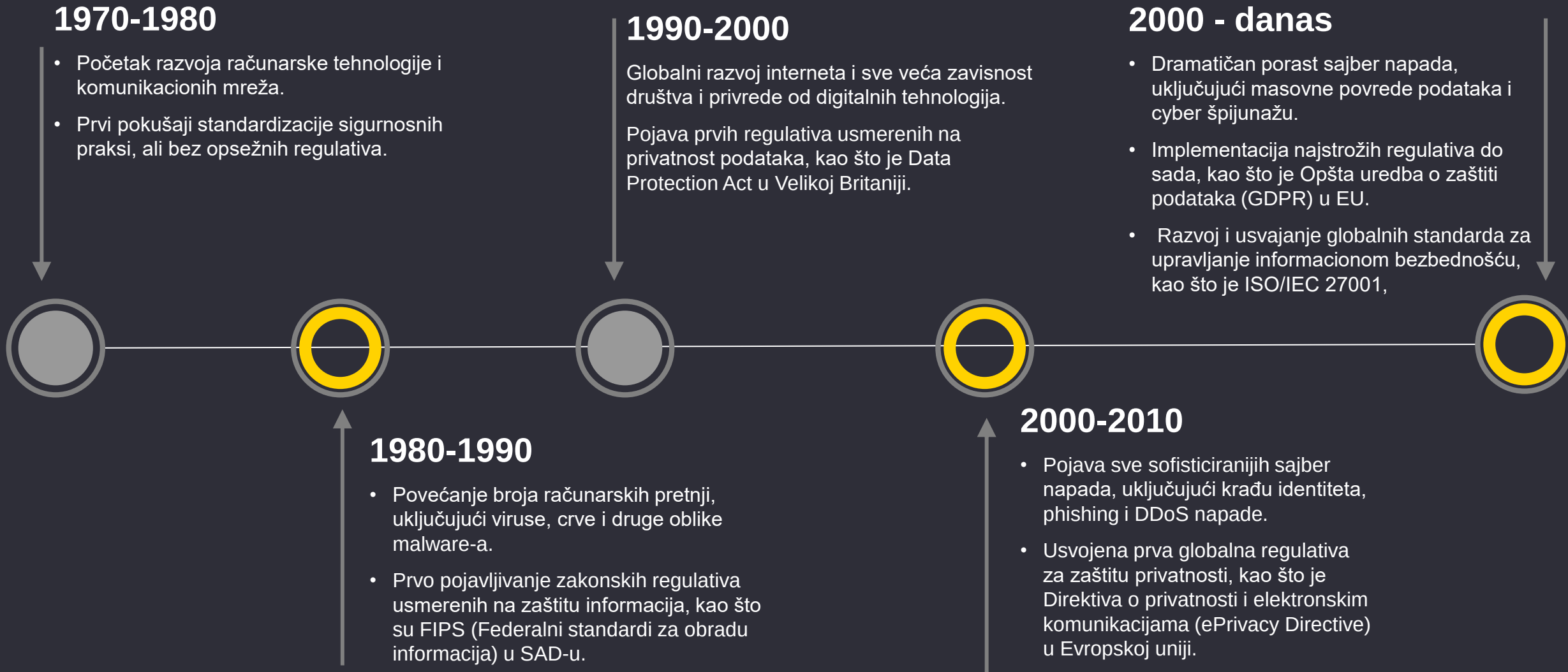
Uloga regulativa i standarda u informacionoj bezbednosti



Regulativa I standard

- **Standard** predstavlja formalni dokument koji sadrži specifikacije, smernice, ili karakteristike koje treba da zadovolji proizvod, proces ili usluga kako bi bio prihvaćen od strane relevantnih strana. Standardi se obično razvijaju u cilju postizanja **univerzalne kompatibilnosti, interoperabilnosti, bezbednosti ili kvaliteta proizvoda ili usluga**.
- **Regulativa** predstavlja zvanični zakonski propis koji postavlja obavezne zahteve, smernice ili standarde koje organizacije, pojedinci ili entiteti moraju da poštuju u određenom kontekstu ili industriji. Regulative se obično uspostavljaju radi zaštite javnog interesa, zaštite potrošača, zaštite životne sredine ili očuvanja javnog reda i mira.
- Definišu najbolje prakse i zahteve za određenu oblast, kao što je upravljanje informacionom bezbednošću (npr. ISO/IEC 27001).
- Organizacije mogu dobrovoljno usvojiti standarde radi unapređenja svojih procesa i praksi.
- Zakonski propisi koji postavljaju obavezne zahteve za organizacije u cilju zaštite podataka i informacija (npr. GDPR).
- Neusaglašenost sa regulativama može rezultirati pravnim posledicama kao što su novčane kazne ili sudski postupci.

Istorijski razvoj regulative I standarda



ISO27001 je prvi put uspostavljen 2005.

Prvi „ransomware“ AIDS Trojan 1989. – PC Cyborg 1.

Maj 2023. – GDPR kazna za META-u, 1.2B USD

**1987. godine napravljen prvi antivirusni program za Atari ST.
1988. je napravljen popis korisničkih adresa naziva Virus na koji su stavljani poznati virusi i načini kako ih ukloniti. John McAfee i Eugene Kaspersky bili su članovi te liste, a kasnije su se istaknuli jer su napravili vlastite antivirusne programe.**

Jan 2025. – DORA stupa na snagu.

Važnost usklađivanja sa regulativama i standardima

Pretnja

Događaj ili faktor sa potencijalom da izazove štetu resursima institucije, kompanije ili organizacije (curenje podataka, narušavanje reputacije, finansijski gubitci...)

Primeri:

Zlonamerni pojedinac ili grupa, štetni kompijuterski program, nepripremljeni zaposleni



Ranjivost

Neuspeh ili slabost procesa koja dovodi do narušavanja bezbednosti koja se može iskoristiti pretnjom.

Primeri:

Nedovoljno jake lozinke, zastareli antivirusni programi



Rizik

Verovatnoća da potencijalna pretnja iskoristi ranjivost, kako bi prouzrokovala štetni uticaj.

Primer:

Izlaganje poverljivih informacija od strane nepažljivog zaposlenog može dovesti do curenja podataka.



Važnost usklađivanja sa regulativama i standardima

1. Zaštita informacija i podataka.

Usklađivanje regulativama i standardima pomaže organizacijama da osiguraju integritet, poverljivost i dostupnost svojih informacija, štiteći ih od gubitaka, krađe ili zloupotrebe

4. Izbegavanje pravnih problema.

Usklađivanje sa regulativama pomaže organizacijama da izbegnu ove probleme, štiteći svoj ugled i finansijsku stabilnost.

2. Smanjanje rizika.

Na ovaj način organizacije identifikuju i smanjuju rizike koji proizilaze iz njihovih operacija, procesa ili proizvoda.

5. Održavanje konkurentnosti

Organizacije koje uspešno primenjuju standarde imaju prednost u odnosu na konkurenciju i mogu lakše zadovoljiti zahteve klijenata ili partnera.

3. Povećanje poverenja korisnika i klijenata

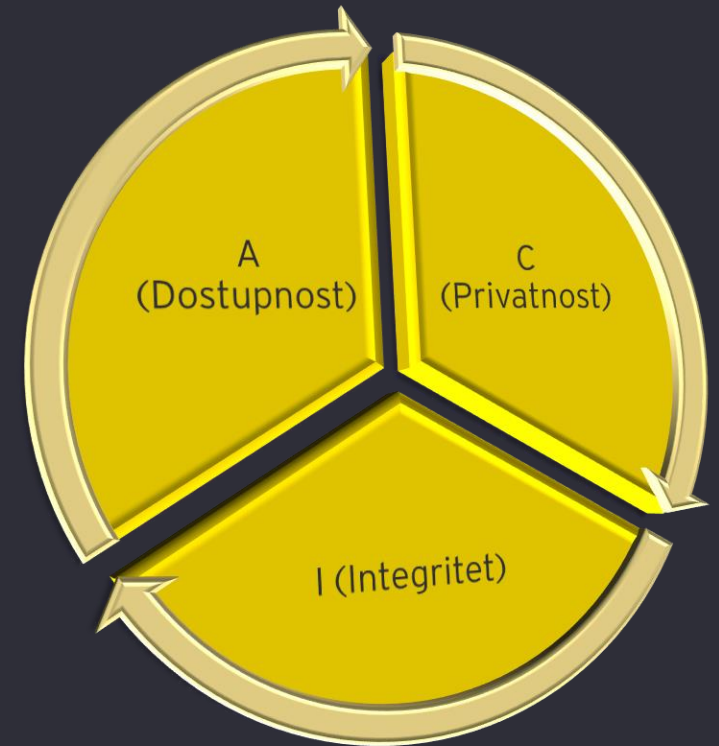
Organizacije usklađene sa relevantnim regulativama i standardima obično izazivaju veće poverenje kod svojih korisnika i klijenata.



Važnost usklađivanja sa regulativama i standardima

1.Osnovni principi usklađenosti:

1. Poštovanje zakona, propisa i regulatornih zahteva koji se odnose na informacionu bezbednost
2. Zaštita organizacije od finansijskih gubitaka, reputacionih šteta i drugih posledica neusklađenosti.
3. Unapređenje poslovne efikasnosti i produktivnosti kroz primenu najboljih praksi u oblasti informacione bezbednosti.



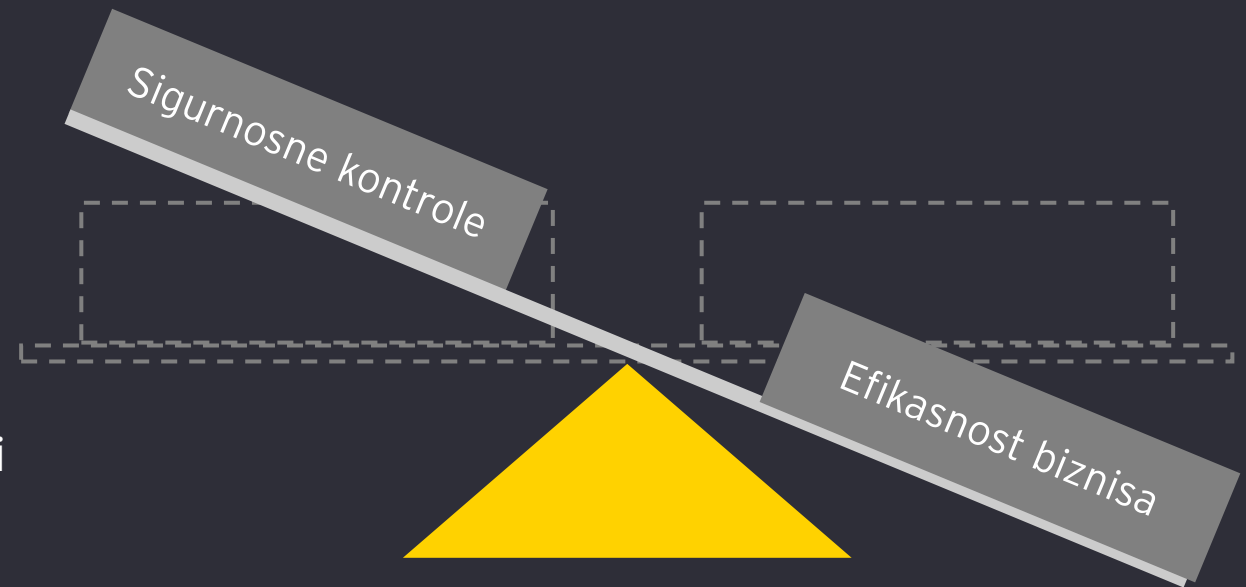
Važnost usklađivanja sa regulativama i standardima

Prednosti usklađenosti:

1. Poboljšana zaštita podataka i informacija od sajber pretnji i incidenata.
2. Povećano poverenje korisnika i klijenata u organizaciju.
3. Smanjenje rizika od finansijskih gubitaka, kazni i sudskih tužbi.

Integracija usklađenosti u poslovne procese:

1. Kontinuirano praćenje promena u regulativama i standardima kako bi se osigurala kontinuirana usklađenost.
2. Implementacija odgovarajućih politika, procedura i kontrola zaštite informacija.
3. Održavanje efikasnosti poslovnih procesa.



Uloga sertifikacija i sertifikacionih tela

Sertifikacije, sertifikaciona tela i revizorske kuće igraju ključnu ulogu u domenu informacione bezbednosti pružajući potvrdu da organizacije, proizvodi ili pojedinci ispunjavaju određene standarde ili zahteve u vezi sa bezbednošću informacija.

Ključne uloge su:

- 1** Potvrda usklađenosti sa standardima sa nezavisne strane
- 2** Povećanje poverenja
- 3** Unapređenje reputacije
- 4** Podsticanje kontinuiranog unapređenja
- 5** Međunarodno priznanje

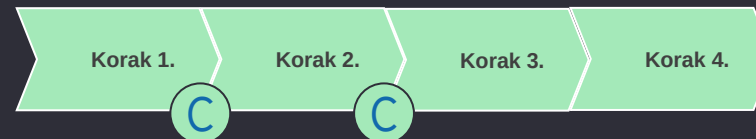
Sertifikacije i regulative

Sertifikacija i standardizacija

Sprovođenje poslovnog procesa



Standardizacija poslovnog procesa



Sertifikaciono telo



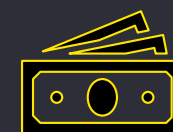
Regulativa

Kompanija

Klijenti



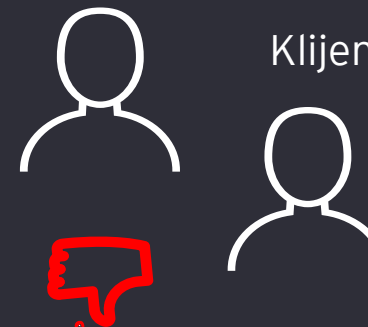
Regulator



Kazna

Kompanija

Klijenti



Revizije trećih strana

Finansijsko izveštanje

Praksa koja je započeta u 19. veku



Direktor

Vlasnik

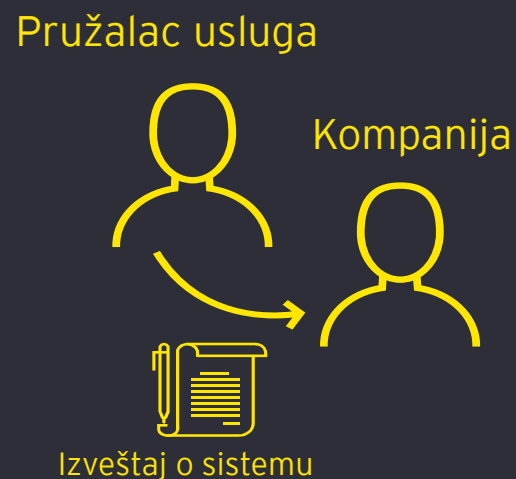
Revizor

Vlasnik

Revidiran finansijski izveštaj

Izveštavanje o sistemima (SOCR)

Praksa koja je započeta 90tih godina



Pružalac usluga

Kompanija

Revizor

Kompanija

Revidiran izveštaj o sistemima

Primer izveštaja revizije treće strane

Ernst & Young LLP
The Ruby, 15th Floor,
29 Senapati Bapat Marg,
Dadar (West),
Mumbai - 400 028, India
Tel: +91 22 6192 0000
Fax: +91 22 6192 1000
www.ey.com

Independent Service Auditor's Report

To the Board of Directors of CLIENT

Scope

We have examined CLIENT's "XX" accompanying Description of XX's Software Service (SaaS) Development, Maintenance, and Optimization Services for Cloud Speech products relevant to the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality, and the Health Insurance Portability and Accountability Act Security Rule for the period 1 January 2016 through 31 December 2016 (Description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy updated as of July 1, 2015 (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability, processing integrity, and confidentiality principles set forth in the AICPA's TSP section 100, Trust Services Principles, and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) throughout the period 1 January 2016 to 31 December 2016. We have also examined the suitability of the design and operating effectiveness of controls to meet the security requirements set forth in the Health Insurance Portability and Accountability Act Security Rule (HIPAA Security Rule requirements). The Description indicates that certain applicable trust services criteria and the HIPAA Security Rule requirements specified in the Description can be met only if Complementary User Organizations Controls contemplated in the design of XX's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such Complementary User Organizations Controls.

XX uses "EdgeConneX, Amazon Web Services, and Equinix, Inc. (subservice organization) to provide Data Center Physical Security and Environmental Safeguards

Description of Systems provided by CLIENT

Overview of Operations

CLIENT "XX" is a global provider of a cloud-based customer engagement platform and applications that use big data and predictive analytics to understand customer intent and drive better service and sales results for large enterprises. The CLIENT Engagement Platform ("the XX platform") enables intuitive sales and service experiences for customers across an enterprise's web, mobile, IVR, social, chat, and voice channels.

XX works with Global 500 enterprises in the retail, healthcare, technology, and travel industries. XX centers located in LOCATION 1, India, LOCATION 5, LOCATION 6, and LOCATION 7. LOCATION 8, and LOCATION 9.

Platform

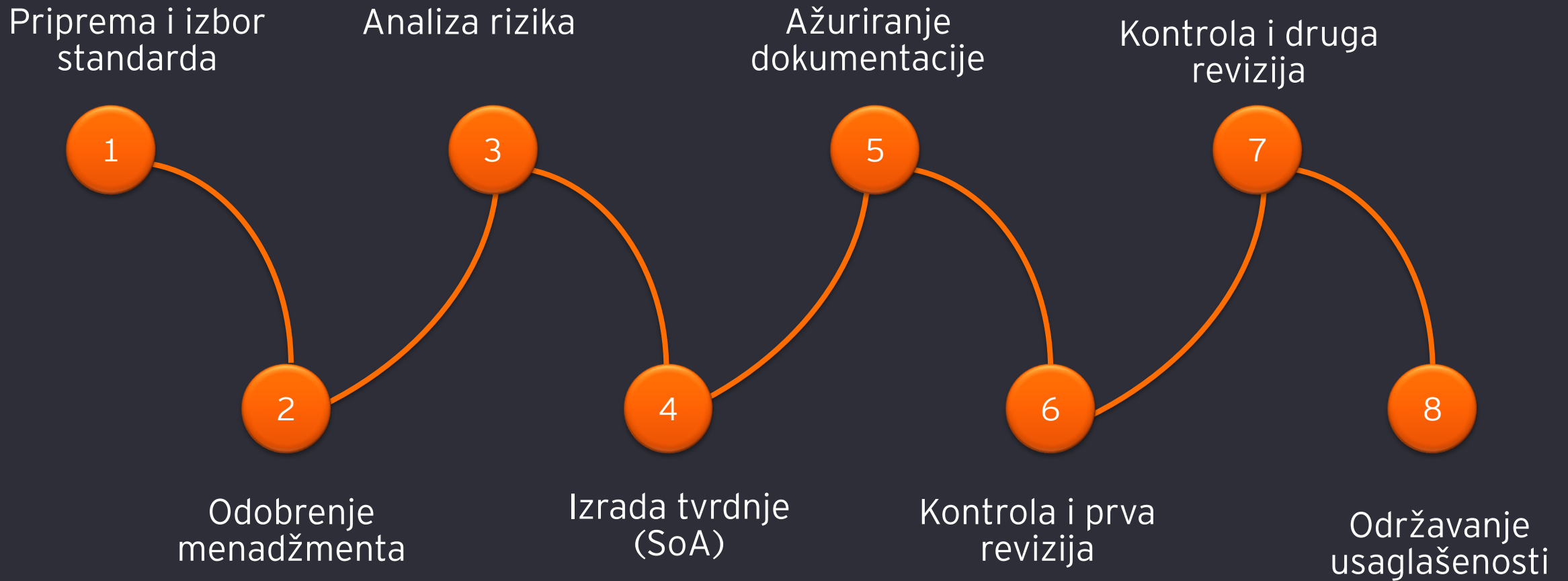
XX deliver products and solutions built and platform uses omni-channel prediction, real-time to understand customer intent and provide service journeys. The products, described guided self-service and agent-assisted in

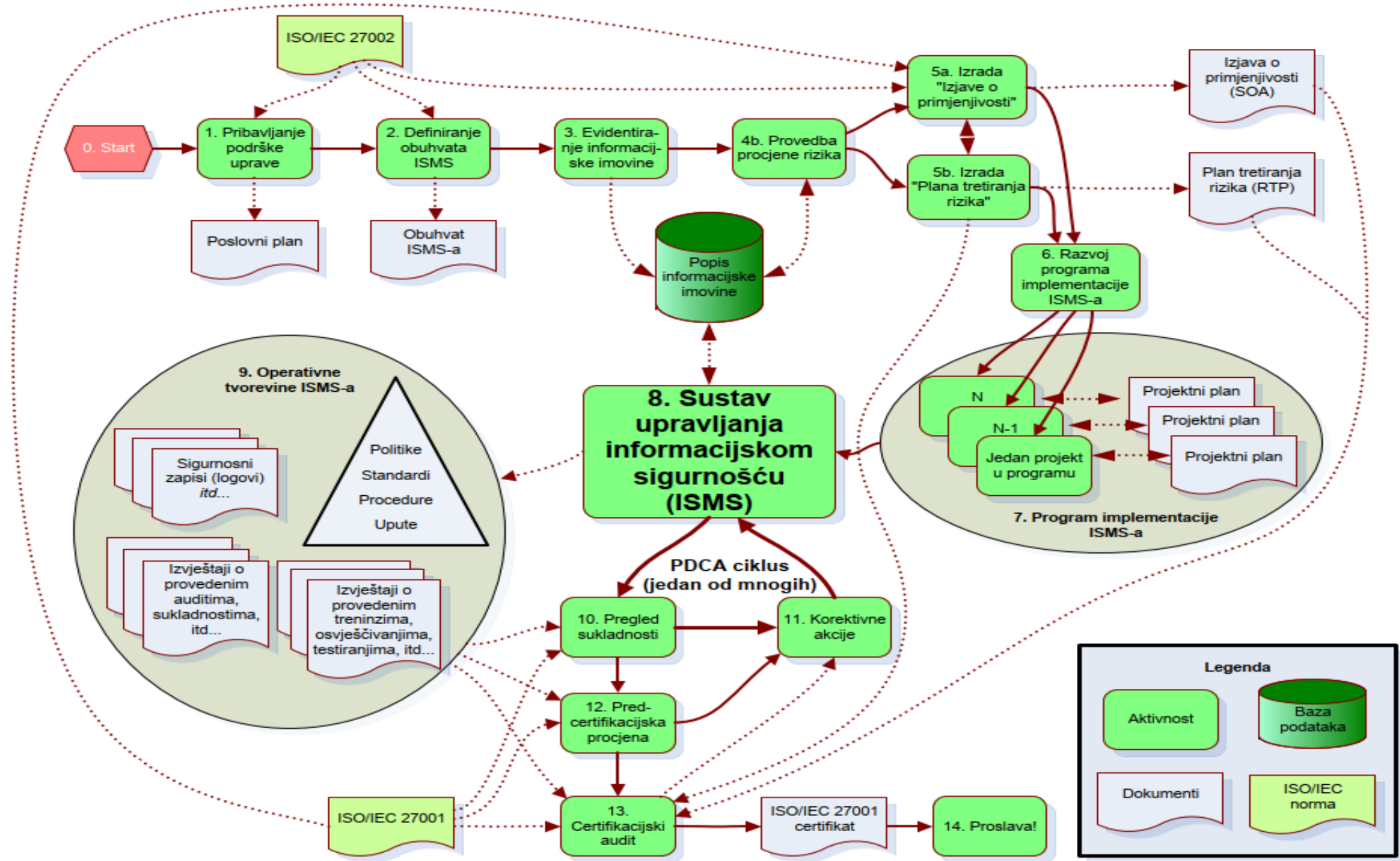
XX Speech

XX Speech is both a self-service IVR smarter, more engaging, and complete online channels. It provides a self-integrated with your online and mobile to natural language, one in which draws upon a customer's web, optimal, data-driven conversation

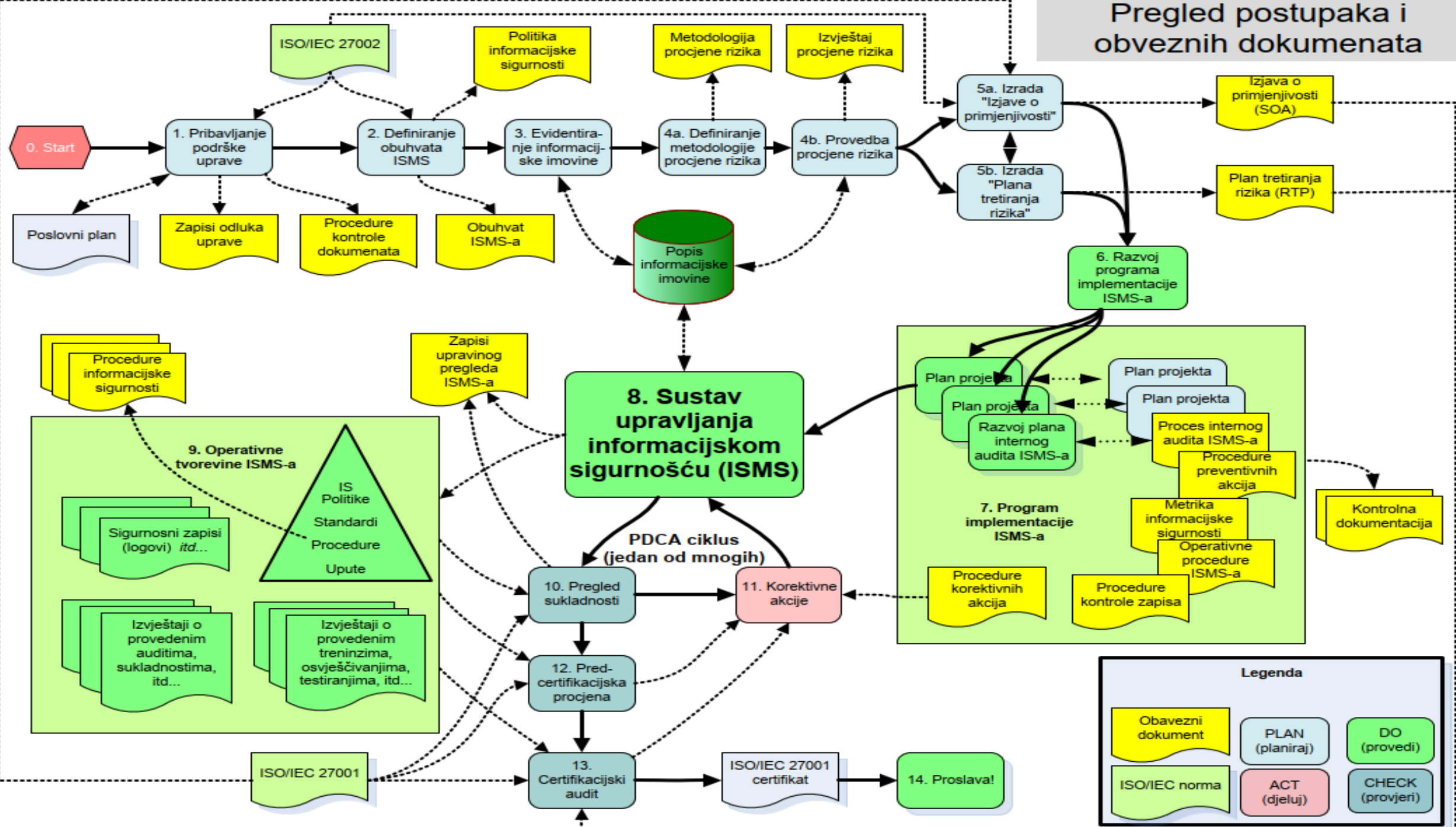
Applicable Trust Services Criteria	Criteria	HIPAA Reference	HIPAA Security Rule Specifications	Controls specified by XX	Testing performed by Ernst & Young	Results of tests
CC1.0 - Common Criteria related to Organization and Management						
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, processing integrity and confidentiality.	\$164.308(a)(2)	Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	XX has organization charts that define organizational structures, reporting lines, authorities, and responsibilities to help meet its commitments and requirements related to system security, availability, processing integrity, and confidentiality.	Inspected the XX's Organization Chart to determine whether XX has defined an <u>organizational structures</u> , reporting lines, authorities, and responsibilities.	No deviations noted.
				Roles and responsibilities are defined in written job descriptions to assign responsibility for security, availability, processing integrity, and confidentiality.	Inspected job descriptions maintained by Human Resources Group to determine whether roles and responsibilities were defined within job descriptions.	No deviations noted.
				The CISO Organization is responsible for developing, maintaining, and publishing the Information Security standards, policies, procedures, and guidelines including policies related to HIPAA Security Rule. The roles and responsibilities of the CISO are documented within	Inspected the Information Security Roles and Responsibilities Policy to determine whether the XX has assigned responsibility for the Information Security to the CISO Organization to oversee the development, implementation, monitoring,	No deviations noted.

Proces sertifikacije





Pregled postupaka i obveznih dokumenata



Ključni standardi

1. ISO 27k serija

Međunarodni standard za upravljanje informacionom bezbednošću.

Definiše zahteve za uspostavljanje, sprovođenje, održavanje i stalno unapređenje sistema upravljanja informacionom bezbednošću.

2. PCI-DSS

Set sigurnosnih standarda uspostavljen od strane PCI Security Standards Council-a radi zaštite podataka o plaćanju.

3. SWIFT CSCF

Set sigurnosnih kontrola razvijen od strane SWIFT-a za korisnike kako bi se poboljšala sigurnost transakcija preko SWIFT mreže.

4. SOCR

Standard koji definiše načine na koje organizacija odgovara na zahteve kriterijuma: Security, Availability, Processing Integrity, Privacy, Confidentiality.

Dodatno će biti analizirani MITTRE ATT&CK i COBIT okviri

Ključne regulative

1. NIS2 direktiva

Evropska direktiva koja postavlja minimalne zahteve za poboljšanje bezbednosti informacionih sistema u ključnim sektorima.

2. GDPR

Opšta uredba o zaštiti podataka koja postavlja stroge zahteve za prikupljanje, obradu i zaštitu ličnih podataka građana EU.

2. DORA

Predložena EU regulativa koja se fokusira na operativnu otpornost digitalnih usluga, uključujući standarde za bezbednost informacionih sistema i incidentni odgovor.

2. Minimalni standardi

Minimalni standardi upravljanja informacionim sistemima finansijskih institucija u Republici Srbiji.

Ključni procesi upravljanja informacionom bezbednošću

1. Upravljanje korisničkim pristupom

2. Upravljanje promenama u sistemu

3. Upravljanje Razvojem softvera

4. Upravljanje bezbednosnim incidentima

5. Upravljanje bezbednosnim operacijama

6. Upravljanje rizicima informacione bezbednosti

7. Zaštita podataka

8. Nadzor i upravljanje informacionim sistemom

8. Upravljanje sigurnosnim zakrpama

9. Upravljanje Resursima informacionog sistema

10. Upravljanje fizičkom bezbednošću

11. Upravljanje kontinuitetom poslovanja

12. Upravljanje kontrolom pristupa

