

GABRIJELA JURIĆ
IVAN BAŠIĆ, dr.sc.
GBS-IT d.o.o., Zagreb
gabrijela.juric@gbs-it.com
ivan.basic@gbs-it.com

DOKUMENTACIJSKI PORTAL – MEHANIZAM INTEGRACIJE SUSTAVA KVALITETE I SIGURNOSTI INFORMACIJA

Sažetak

10% prosječnog radnog dana u uredu se potroši na potragu za dokumentima. Sustav upravljanja sigurnošću informacija kao temeljne zahtjeve postavlja dostupnost, cjelovitost i povjerljivost informacija. Zahtjevi koje je postavio QMS na dokumentacijski sustav moraju se nadopuniti i ovim uvjetima. U radu će biti specificirano koje zahtjeve na dokumentaciju integrirajući ova dva sustava treba zadovoljiti i opisan će biti alat koji na jednostavan, efikasan način to zadovoljava. Pri izgradnji integriranog sustava (ISMS i QMS) treba računati povijest organizacije i postojeću dokumentaciju integrirati ali također je sagledavajući s aspekta sigurnosti. Kako bi ISMS i QMS integrirani sustavi zaživjeli u implementaciji potreban je alat koji će osigurati osim zadovoljenja norme i organizacijsku kompatibilnost. Dokumentacijski portal mora na jednostavan način uklapati postojeću dokumentaciju, osigurati atribuciju dokumenata, ključne riječi i mapiranje u bazu znanja, podržavati bilo koji format dokumenta, jednostavno i napredno pretraživanje te podržavati autentifikaciju. Kao jedan od nužnih zahtjeva je i automatsko sigurnosno pohranjivanje (backup) dokumenata. Također potrebna je i tehnička jednostavnost koja zahtjeva standardnu tehnologiju, univerzalnu točku prijave te Web sučelje koje podržava sve browsere.

Ključne riječi: *upravljanje dokumentima, sigurnost informacija, portal*

1. UVOD

10% prosječnog radnog dana u uredu se potroši na potragu za dokumentima. Sustav upravljanja sigurnošću informacija kao temeljne zahtjeve postavlja dostupnost, cjelovitost i povjerljivost informacija. Zahtjevi koje je postavio QMS na dokumentacijski sustav moraju se nadopuniti i ovim uvjetima. Pri izgradnji integriranog sustava (ISMS i QMS) treba računati povijest organizacije i postojeću dokumentaciju integrirati ali također je sagledavajući s aspekta sigurnosti. Kako bi ISMS i QMS integrirani sustavi zaživjeli u implementaciji potreban je alat koji će osigurati osim zadovoljenja norme i organizacijsku kompatibilnost. Dokumentacijski portal mora na jednostavan način uklapati postojeću dokumentaciju, osigurati atribuciju dokumenata, ključne riječi i mapiranje u bazu znanja, podržavati bilo koji format dokumenta, jednostavno i napredno pretraživanje te podržavati autentifikaciju. Kao jedan od nužnih zahtjeva je i automatsko sigurnosno pohranjivanje (backup) dokumenata. Također potrebna je i tehnička jednostavnost koja zahtjeva standardnu tehnologiju, univerzalnu točku prijave te Web sučelje koje podržava sve browsere

2. ZAHTJEVI SUSTAVA KVALITETE I SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

2.1. Zahtjevi norme ISO 9001 na dokumentaciju i zapise

Dokumentima koje zahtijeva sustav upravljanja mora se upravljati. Mora se uspostaviti dokumentirani postupak koji definira potrebno upravljanje za:

- odobranje primjerenosti dokumenata prije objavljivanja,
- pregled i osuvremenjivanje kada je potrebno i ponovno odobranje dokumenata,
- osiguravanje označavanja izmjena i statusa najnovijeg izdanja dokumenata,
- osiguravanje dostupnosti odgovarajuće verzije dokumenata na mjestu uporabe,
- osiguravanje trajne čitljivosti dokumenata i njihovo brzo prepoznavanje,
- osiguravanje da dokumenti vanjskog porijekla budu označeni te da se upravlja njihovom raspodjelom,
- sprečavanje nenamjerne uporabe zastarjelih dokumenata te primjereno označavanje ako se čuvaju iz bilo kojeg razloga

Zapisi moraju biti uspostavljeni i održavani kako bi se osigurao dokaz o sukladnosti sa zahtjevima i učinkovitim provođenju sustava upravljanja. Zapisi moraju ostati čitljivi, lako se prepoznavati i pronalaziti. Mora biti uspostavljen dokumentirani postupak koji određuje potrebno upravljanje za označavanje, pohranu, zaštitu, pronalaženje, vrijeme čuvanja i dostupnost zapisa.

2.2. Zahtjevi norme ISO 27001 na dokumentaciju i zapise

Dokumenti zahtijevani ISMS (sustavom upravljanja sigurnošću informacija) moraju biti štice i kontrolirani. Mora se uspostaviti dokumentirani postupak koji definira potrebno upravljanje za:

- odobranje primjerenosti dokumenata prije objavljivanja
- pregled i osuvremenjivanje kada je potrebno i ponovno odobranje dokumenata,
- osiguravanje označavanja izmjena i statusa najnovijeg izdanja dokumenata
- osiguravanje dostupnosti odgovarajuće verzije dokumenata na mjestu uporabe
- osiguravanje trajne čitljivosti dokumenata i zakonitosti
- osiguravanje da dokumenti vanjskog porijekla budu identificirani
- osiguravanje da je kontrolirana distribucija dokumenata
- sprečavanje nenamjerne uporabe zastarjelih dokumenata
- primjena odgovarajuće identifikacije zastarjelih dokumenata, ako se čuvaju iz bilo kojeg razloga

Zapisi moraju biti uspostavljeni i održavani kako bi se osigurao dokaz o sukladnosti sa zahtjevima i učinkovitim provođenju ISMS-a.

Zapisi moraju biti kontrolirani. ISMS mora uzeti u obzir svaki važeći zakonski propis. Zapisi moraju biti zakoniti, čitljivi, lako se prepoznavati i pronalaziti. Kontrole za identifikaciju, pohranjivanje, zaštitu, vrijeme zastarijevanja, ponovno pronalaženje i način odlaganja zapisa mora biti dokumentiran

Ako promotrimo ova dva pristupa vidjet ćemo da su u mnogo čemu slična, ali dok ISO 9001 traži prvenstveno pristupačnost dokumenata i njihovu ažurnost ISO 27001 je više orijentiran na samu povjerljivost informacije – bilo da je ona pohranjena u zapisima ili u dokumentima.

Zbog razloga povjerljivosti informacije potrebno je naći rješenje koji će integrirati laku dostupnost i prepoznatljivost s pravom pristupa.

Također važan aspekt ISMS a je i legislativa – koja nije bila toliko provjeravana u QMS sustavima.

Dok je ISO 9001 se brinuo o distribuciji – ISO 27001 se brine i o povjerljivosti distribuiranih dokumenata. Više nije dovoljna distribucijska lista na koju će se ljudi potpisati – potrebno je sagledati da povjerljivi dokumenti i tijekom uporabe imaju posebne postupke. Papirnata rješenja više ne zadovoljavaju – kompleksnost upravljanja povjerljivim informacijama se multiplicira

3. INTEGRACIJA DOKUMENTACIJE ISMS-A I QMS-A

3.1. Struktura

Novina u ISMS-u u odnosu na QMS je postojanje elementarnih politika kao nužnih u samoj piramidi dokumentacije. Politike sigurnosti i kvalitete zajedno sa ostalim strateškim dokumentima su na vrhu piramide.

Kako bi se integrirali sustavi u poslovanje poslovnici kvalitete i sigurnosti su druga razina – međutim ISMS tu postavlja svoje zahtjeve – pa u drugu razinu idu i važeći zakonski propisi.

Na ovaj način je u strukturu unesen zahtjev na usklađenost dokumenata s zakonom.

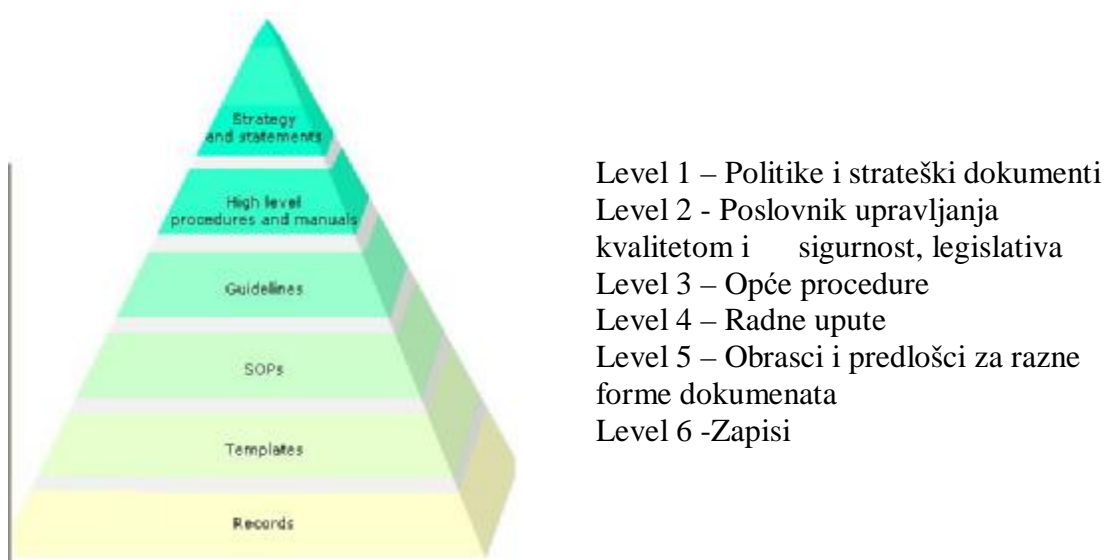
Ova razina je razina integracije ova dva sustava – zajedno su obavezne procedure QMS sustava (Korektivne radnje, Preventivne radnje, Unutarnja neovisna ocjena, Upravljanje dokumentima, Upravljanje zapisima, Upravljanje nesukladnim proizvodom) i elementarne politike ISMS-a. Kako bi se oba sustava integrirala u poslovanje na ovu razinu su dodani i poslovna uputstva (npr. Način nominacije projekata) – namijenjena managementu.

Slijedeća razina dokumentacije su radne upute iz QMS-a i kontrole tražene ISMS-om – jer kontrole u ISMS-u upravo to i jesu – radna uputstva koja se u različitim segmentima koriste u svakodnevnom radu.

Zbog jednostavnosti korištenja predlošci i obrasci su zasebno odvojeni – te je zadnja razina zapisi.

Struktura zapisa je vrlo ovisna o organizacijskom ustrojstvu tvrtke.

Slika 2: Primjer strukture dokumentacijskog portala



Povjerljivost, cjelovitost i dostupnost informacija

Sigurnost informacija :Očuvanje povjerljivosti, integriteta i dostupnosti informacije.

- **Povjerljivost:** Informacija je dostupna samo osobama kojima je i namijenjena
- **Cjelovitost:**Točnost i sadržajnost informacije mora biti zaštićena
- **Dostupnost** Autorizirani korisnici moraju moći pristupiti informaciji kada im je potrebna

Ovo su temeljne definicije samog pojma sigurnosti. Kako se odnose na cijeli sustav odnose se i na dokumentaciju sustava.

Povjerljivost – za zadovoljenje ovog zahtjeva je potrebno imati autentifikaciju na dokumentacijski sustav. Ostajanje na papirnatom rješenju multiplicira upravljanje distribucijskim listama – do razine neodrživosti sustav.

Cjelovitost – Sigurnost da je informacija točna i potpuna – zahtjeva verzioniranje i pristup prošlim verzijama – također traži nemogućnost promjene sadržaja. Koliko puta sete vidjeli da se ispisuje jedna strana dokumenta i samo zamjenjuje? Takav postupak je ISMS-om zabranjen – cjelovitost informacije mora biti očuvana.

Dostupnost: - ovo je zahtjev koji se traži i u ISO 9001 – međutim ISMS- traži da se informacije pohranjuju (zapisi) kako bi se mogli povratiti u slučajevima nesreće. Dakle – morate imati sustav koji neće izgoriti (papirnati oblik) ili se srušiti bez povratka (dokumentacijski sustavi):

- Lako nalaženje: atribucija dokumenata i ključne riječi u terminima dostupnosti postaju jako važne. Također pretraživanje po cijelom tekstu omogućava nepotrebnost pamćenja naziva dokumenta
- Distribucija: kako ISMS ne dozvoljava slanje povjerljivih dokumenata elektronskom poštom potrebno je imati sustav notifikacije o promjenama na dokumentu pa da se korisnik dokumenta sam prijavi na sustav i sagleda promjene
- Označavanje: Govoreće šifre su i dalje ljudskom rodu primjerene – ali ih treba automatizirati ovisno o već definiranoj strukturi dokumentacije
- Verzioniranje: dostupnost samo posljednje verzije nije više dovoljna, ali je potrebno osigurati da se stare verzije više ne upotrebljavaju te da nisu dostupne i dalje po pravilima o povjerljivosti

4. ZAKLJUČAK: ZAHTJEVI NA DOKUMENTACIJSKI PORTAL

Usklađenost s ISO 9001 sustavom upravljanja kvalitetom

- Jednostavan način uklapanja postojeće dokumentacije
- Atribucija dokumenata, ključne riječi i mapiranje u bazu znanja
- Notifikacija o promjenama u dokumentu
- Podržavanje bilo kojeg formata dokumenta
- jednostavno i napredno pretraživanje
- Verzioniranje, jedinstvenost zadnje verzije i čuvanje starih verzija (opcionalno)
- Razine dokumentacije usklađene sa sustavom ISO 9001

Usklađenost s ISO 27001 sustavom upravljanja sigurnošću informacija

- Podržava autentifikaciju
- Razine dokumentacije usklađene sa sustavom ISO 27001

- Razrađen sustava dozvola pristupa i objavljivanja
- Pohranjivanje zapisa

Tehnička jednostavnost

- Standardna tehnologija – koja ne zahtjeva instalaciju kompliciranih softwera i hardwera – jer kompleksnošću se povećava ranjivost sustava
- Univerzalni enter point – kako bi se omogućila jednostavnost autentifikacije
- Web sučelje koje podržava sve browsere
- Automatsko sigurnosno pohranjivanje (backup) dokumenata

LITERATURA

- [1] ISO 27001: Information Security Management - Specification With Guidance for Use
- [2] BS 7799-2:2000: Information Security Management Sysrtems - Specification With Guidance for Use
- [3] ISO 9001:2000: Sustav upravljanja kvalitetom- zahtjevi
- [4] The Art and Science of Documentation Management, Graziella Tonfoni, Lakhmi Jain

DOCUMENTATION PORTAL –INTEGRATION MECHANISM OF QUALITY AND INFORMATION SECURITY SYSTEMS

Summary

Approximately 10% of the average work day is spent on looking for documents. Fundamental requirements of information security management systems are availability, integrity and confidentiality of information. Regarding this requirements set by QMS on documentation system have to be upgraded. Specification of documentation requirements set by integration of this two systems and a efficient tool which is simple to use and maximally supports it, will be described later in the paper. History of organization and existing documentation have to be considered from security point of view in development of such integrated system. Organizational compatibility is one of necessities provided by documentation portal in order to successfully implement ISMS and QMS. Simple fit for existing documentation on file servers, supporting any documentation format, user-friendly document attribution, support for key words and mapping in knowledge base, enabling simple and advanced (full text) content search and supporting authentication are requirements for such documentation portal. One of mandatory requirements is security backup. Technical simplicity is an advantage of such tool.

Key words: *control of documents, information security, portal*