KAKO

OBVLADOVATI ORGANIZACIJSKA TVEGANJA S POMOČJO CERTIFICIRANJA SISTEMOV VODENJA

BUREAU VERITAS

OBVLADOVANJE TVEGANJA

za hitro spreminjajoči se svet

Vsebina

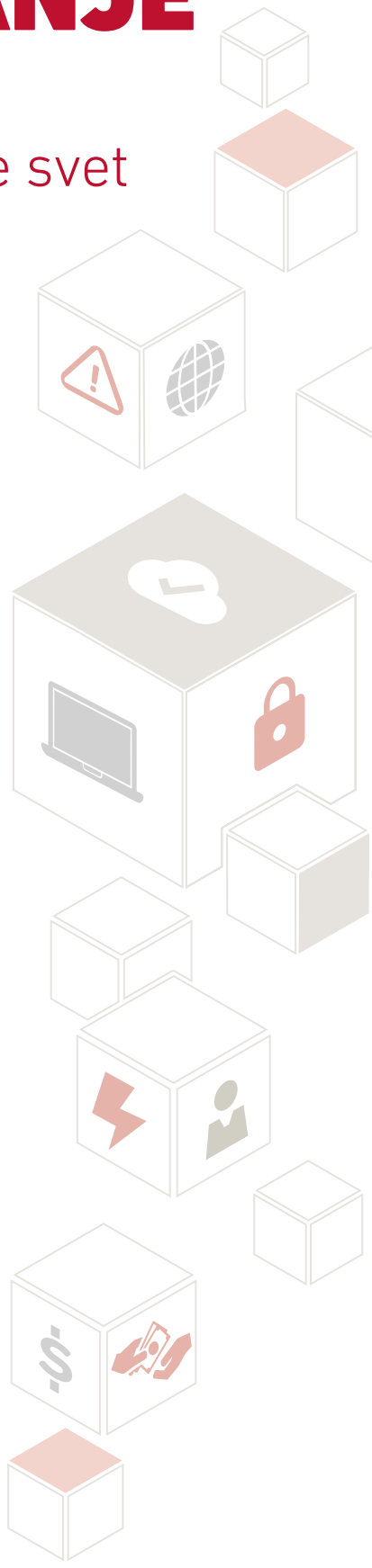
Stran 1
Uvod

Stran 2-3
Pet nastajajočih tveganj za podjetništvo

Stran 4-6
Oblikovanje okvirja za obvladovanje tveganja

Stran 7-9
Certificiranje za obravnavanje specifičnih tveganj

Stran 10
Usposabljanje in certificiranje



Organizacije danes, se v primerjavi s preteklostjo, soočajo s povečanim številom tveganj, saj digitalizacija premoženja, izdelkov in storitev ustvarja priložnosti, vendar tudi grožnje kibernetski varnosti. Vlade poskušajo področje regulirati z uvedbo predpisov za področja, ki segajo od zaščite podatkov do korupcije. Tradicionalne grožnje neprekinjenemu poslovanju, na primer prekinitve pri izvajanju javnih služb, so se zaradi naše odvisnosti od digitalnih mrež skokovito povečale. Organizacije navadno upravljajo s tveganji, ki jih razumejo, na primer finančno, gospodarsko in poslovno tveganje. A nastajajoča, kompleksna narava drugih groženj, posebej tistih, ki so povezane s podatki, premoženjem in ljudmi, pogosto povzroči, da se ta tveganja izmuznejo nadzoru številnih menedžerjev.

Potrebna je celovita strategija, da prepoznamo tveganja na področju poslovanja, in nato, da jih z doslednim izvajanjem definiranih procesov v sistematičnem okviru obvladujemo. To je edini način, da dobite 360-stopinjski pogled na tveganje, spodbudite proaktivno kulturo obvladovanja tveganj, zavarujete svoj ugled, si zagotovite zaupanje deležnikov in zaščitite svoje delovanje.

Ta bela knjiga na kratko predstavlja celovit pristop za obravnavanje podjetniških tveganj, da bi odgovorila na specifične zahteve vaše organizacije.

5 TVEGANJ,
zaradi katerih menedžerji ne spijo

1. **78%** **VARNOST INFORMACIJ**
2. **78%** **NEPREKINJENOST POSLOVANJA**
3. **68%** **ZAŠČITA PODATKOV ODJEMALCEV**
4. **53%** **SLABA ZAŠČITA ALI RABA PREMOŽENJA**
5. **52%** **KORUPCIJA MED ZAPOSLENIMI ALI V DOBAVNI VERIGI**

ŽENETA JIH
2 GLAVNI SKRBI

UGLED

je ključno vodilo,
ko razmišljamo o

zaščiti podatkov odjemalcev 40%

varnosti informacijskih sistemov 36%

POSLOVNA USPEŠNOST

je ključno vodilo za

neprekinjeno poslovanje 73%

tveganja pri upravljanju premoženja 67%

ORGANIZACIJE SO ZAČELE
OBRAVNAVATI TA TVEGANJA

6 od 10

organizacij ima vzpostavljenih eno ali več politik ali postopkov, ki pokrivajo:

→ **Varovanje podatkov**

→ **Varnost informacijskih sistemov**

→ **Nepretrgano poslovanje**

4 od 10

organizacij je vpeljalo:

→ **sistem vodenja za varovanje podatkov**

ISO 27001

in/ali

→ **sistem vodenja neprekinjenega poslovanja**

ISO 22301

1 od 3

organizacij svoje sisteme varovanja informacij upravlja s pomočjo certifikata **ISO 27001** ali podobnega standarda

Certificiranje sistema vodenja za organizacijsko tveganje prinaša

3 KLJUČNE PREDNOSTI

Zagotavlja DOSLEDNO UPORABO vaših sistemov vodenja

Usmerjeno je v SKLADNOST in ščiti ugled

Dosega NENEHNO IZBOLJŠEVANJE

Glede na anketo, ki jo je izvedel Bureau Veritas poleti 2017

OBLIKOVANJE CELOSTNEGA OKVIRA

za obvladovanje organizacijskih tveganj

VSAKA POSLOVNA DEJAVNOST VKLJUČUJE DOLOČENO TVEGANJE.

Organizacije prepoznavajo, spremljajo in upravljajo tista tveganja, za katera verjamejo, da so ključna za njihovo poslovanje. V ospredju so navadno finančna, tržna in regulativna tveganja; operativna tveganja, kakršni sta varnost in dobavna veriga, pa veljajo za bolj ali manj kritična, odvisno od narave poslovanja. Upoštevajo tudi katastrofe, na primer ekstremne vremenske razmere in izpade energije.

A v današnjem hitro spreminjajočem se svetu potencialni učinek in verjetnost za tveganja naraščata, tradicionalno združena v skupino operativnih ali regulativnih tveganj ali izrednih dogodkov (glejte str. 5). Organizacije se morajo spoprijemati z grožnjami kibernetskih napadov in izpadov informacijske tehnologije, in z njihovim potencialnim učinkom na ugled in neprekinjeno poslovanje. Vedno strožje so tudi uredbe, posebej na področjih, kakor so protikorupcijsko delovanje in zaščita podatkov. Po drugi strani pa lahko v tem izrazito tekmovalnem okolju do nadpovprečne uspešnosti pridemo s proaktivnim upravljanjem poslovnega premoženja.

POGLED 360° S CELOSTNIM OKVIROM OBVLADOVANJA TVEGANJ

Že sam obseg in kompleksnost nastajajočih tveganj vodjem otežuje, da bi bili na tekočem z grožnjami, s katerimi se soočajo njihove organizacije. Zato je učinkovito obvladovanje tveganj najbolje doseči skozi kompleksen okvir, ki zagotavlja temelje in dogovore, s pomočjo katerih ga bomo na vseh ravneh vpeli v organizacijo. Obvladovanje tveganj ne more biti izolirana dejavnost, ločena od glavnih postopkov organizacije. Voditi ga mora najvišje vodstvo in biti mora neločljiv del celotne organizacije, vključno s strateškim načrtovanjem in projekti ter s spremembami v procesih vodenja. Prav tako mora biti prikrojeno potrebam organizacije in njenemu kontekstu. Za veliko banko bo zaščita podatkov odjemalcev verjetno med glavnimi tveganji. Upravljanje premoženja je večja skrb za industrijskega proizvajalca električnih generatorjev kakor, denimo, za oglaševalsko agencijo.

Noben okvir ni zacementiran: odzivati se mora na zunanje in notranje dogodke in na spremembe v kontekstu in znanju. Ko se grožnje in priložnosti pojavijo ali pridobijo na pomembnosti, morajo upravljavci tveganj znati spremljati, pregledati in ponovno oceniti obstoječi okvir in zagotoviti, da ostane dinamičen, iterativen in relevanten.

Z razvijanjem, uvajanjem in nepretrganim izboljševanjem okvirja za integriranje obvladovanja tveganj v splošno upravljanje, strategijo, načrtovanje, postopke poročanja, politike, vrednote in kulturo organizacije zagotavljajo, da odločitve obvladovanja tveganj temeljijo na najboljših razpoložljivih podatkih. To odločevalcem pomaga, da se ustrezno odločijo, dajo določenim dejanjem prednost, razlikujejo med alternativnimi poteki dogajanja in ustvarjajo odgovornost.

> *Že sam obseg in kompleksnost nastajajočih tveganj menedžerjem otežuje možnost, da bi bili na tekočem z grožnjami, s katerimi se soočajo njihove organizacije.*

Razvrščanje tveganj po pomembnosti

KIBERNETSKA VARNOST JE NAJPOMEMBNEJŠE NASTAJAJOČE ORGANIZACIJSKO TVEGANJE ZA VELIKE ORGANIZACIJE

Da bi videli, kako vodilne organizacije tveganja razvrščajo po pomembnosti, smo pogledali glavna tveganja, povzeta v izboru desetih organizacij, uvrščenih na FTSE 100.[1] Naš cilj je bil ugotoviti, katera tveganja so najpogosteje navedena, in če nastajajoča organizacijska tveganja[2] veljajo za glavna tveganja in jih tako obravnavajo. Spodnji diagram prikazuje tveganja, ki smo jih identificirali v vzorcu.[3] Zaradi jasnosti smo tveganja združili pod skupne naslove. Kakor bi lahko pričakovali, so bila najpogostejša tveganja, s katerimi so se srečevale organizacije, povezana z možnostjo za neposreden vpliv na prodajo in dobiček: uredbe, tržišče, makro in operativna tveganja.

Zanimivo, informacijska varnost in kibernetska varnost sta takoj za njimi. Navedlo ju je devet od desetih preučenih organizacij:[4] ena od organizacij je kot dodatno informacijsko varnostno tveganje navedla zanesljivost IT.

Redno so navajali druga operativna tveganja, vendar ne vedno kot samostojna tveganja. Protikorupcijska dejavnost je bila pogosto omenjena kot del skladnosti s pravili, le redko pa kot izolirano tveganje. Neprekinjeno poslovanje je 7 od 10 organizacij navedlo v razlagi tveganj kot so delovanje ali varovanje podatkov. Upravljanje s premoženjem je bilo najmanjkrat omenjeno operativno tveganje.

O VZORCU

Izbrane organizacije so iz širokega nabora panog: nepremičninske in finančne storitve, rudarstvo, nafta in plin, farmacevtska industrija, transport in letalska industrija, telekomunikacije, mediji in oglaševanje, trgovina na drobno, prehrana. Vse so multinacionalke. Povprečno število tveganj, ki so jih identificirale organizacije, je bilo 10,7.

- Nastajajoča podjetniška tveganja, ki jih lahko obravnavamo s pomočjo novih certifikatov, omenjenih v tej beli knjigi.
- Tveganja, ki jih lahko obravnavamo s pomočjo obstoječe sheme certificiranja, preverjanja poročil o emisijah in poročil o zagotovitvah trajnosti.
- Druga tveganja

[1] Organizacije v Združenem kraljestvu, ki kotirajo na borzi, so dolžne analizirati in razkriti svoja glavna tveganja kot del letnega finančnega poročila, vključno s tistimi, ki bi grozila njihovemu poslovnemu modelu, prihodnji uspešnosti, solventnosti ali likvidnosti.

[2] Spletna varnost, varovanje osebnih podatkov, nepretrgano poslovanje, upravljanje s premoženjem, protikorupcijska dejavnost.

[3] Tveganja v diagramu so razvrščena po velikosti, vendar niso predstavljena v merilu.

[4] Ena od organizacij jih je navedla kot »katastrofično tveganje«.

OBLIKOVANJE CELOSTNEGA OKVIRJA
za obvladovanje operativnih tveganj

UPORABA CERTIFICIRANJA ZA OBVLADOVANJE SPECIFIČNIH TVEGANJ

Eden od problemov, s katerim se organizacije pogosto srečajo, je kako obvladovati operativna tveganja v celotni organizaciji, potem ko so bila enkrat prepoznana kot kritična znotraj okvira obvladovanja tveganja.

V tem kontekstu nam bosta implementacija in certificiranje za mednarodno priznan sistem vodenja za vsako od kritičnih tveganj ponudila koristen način za premostitev vrzeli med visokimi ambicijami in vsakodnevnimi procesi in mišljenjem, ki ga zahteva obvladovanje vsakega tveganja.

Uvajanje sistema vodenja za obvladovanje tveganj ščiti vašo organizacijo, zmanjšuje grožnje dobičku, uspešnosti in ugledu. Certifikat pa zbuja zaupanje v vaše vodenje, tako med zaposlenimi, kakor tudi med zunanjimi deležniki. Pomaga dokazovati skladnost z zakonodajo in mednarodno priznanimi kriteriji in sporoča, da delujete transparentno in ste zavezani odličnosti. Še več, če bi prišlo do kršitev, certifikat kaže na dolžno skrbnost in vam lahko v nekaterih primerih omogoči zmanjšanje kazni.

Tveganja, kritična za delovanje družbe, prepoznamo s pomočjo celostnega spremljanja, ki ga omogoča natančen okvir.

Kako to deluje v praksi? V zgoraj navedenem primeru se lahko vodstvo velike banke odloči, da bo certificiralo svoj sistem vodenja ali pa bo za obravnavanje informacijske varnosti in neprekinjenega poslovanja – prepoznanih neposrednih groženj – prevzelo tehnični standard. Na osnovi rezultatov analiz in ocen tveganja znotraj konteksta organizacije, se lahko vodstvo nadaljnje odloča o potrebi po dodatnih certifikatih, s katerimi bi ta tveganja lažje obvladali (npr.: protikorupcijski certifikat in certifikat za varovanje podatkov).

S tem, da opredelite tveganja, ki zadevajo vašo organizacijo, in se nato z njimi soočite tako, da se ustrezno certificirate, vaša organizacija naredi pomemben korak na poti k odpornejšemu delovanju – in večji umirjenosti.

Do prepoznavanja tveganj, ki so kritična za delovanje, pridemo s celostnim spremljanjem, ki ga omogoča natančen okvir; posamezni certifikati zagotavljajo, da se znamo na resne grožnje organizaciji pravilno pripraviti.

CERTIFIKATI
osredotočeni na kritična poslovna tveganja

Za številna področja se za tveganja že 30 let uporabljajo mednarodni certifikati, prva sta bila certifikat za sistem vodenja kakovosti (ISO 9001) in sistem ravnanja z okoljem (ISO 14001). Naslednja generacija sistemov za obvladovanje tveganj vključuje informacijsko varnost, neprekinjeno poslovanje, upravljanje s premoženjem in protikorupcijsko delovanje, ki jih Bureau Veritas razvršča v skupen portfelj operativnih tveganj. Peto tveganje, varstvo podatkov, je mogoče obvladovati s pomočjo tehničnega standarda, ki ga je razvil Bureau Veritas.

INFORMACIJSKA VARNOST: ISO 27001 ISMS

V današnjem, od tehnologije odvisnem svetu naraščajo grožnje informacijski varnosti. En sam dogodek lahko vpliva na podobo vaše organizacije, neprekinjeno poslovanje in prihodek. Velike organizacije so že dolgo redne tarče napadov, vedno večje pa je tveganje tudi za mala in srednje velika podjetja. Zato se organizacije soočajo s strožjimi pravili, pričakovanja deležnikov glede varovanja podatkov pa so visoka. Vedno več organizacij tako prepoznava vrednost strukturiranega pristopa k informacijski varnosti, kakršnega prinaša ISO 27001.

Certifikat sporoča, da ste zavezani uspešnemu pristopu in vam omogoča, da svojim odjemalcem nudite transparentnost ter jim dokazujete, da odgovorno ravnate z njihovimi podatki. Deležnikom zagotavlja, da ste se sposobni odzvati na izjemne grožnje in na kompleksnosti moderne tehnološke družbe, to pa vam povečuje ugled in vas ločuje od tekmecev.

Za več informacij **kliknite tukaj**.

> *Velike organizacije so že dolgo redne tarče napadov, vedno večje pa je tveganje tudi za mala in srednje velika podjetja.*

Certifikati, osredotočeni na

TVEGANJA, KRITIČNA ZA DELOVANJE

NEPREKINJENO POSLOVANJE: ISO 22301 BCMS

Težave in nedelovanje pri izvajanju javnih služb, izpadi in vdori v informacijsko tehnologijo, naravni pojavi, motnje v dobavni verigi: v našem negotovem svetu so to le nekatere od številnih groženj, ki vam lahko škodujejo – ali vas uničijo – tako da ogrozijo vašo dobavno verigo, standarde kakovosti ali varnost vaše organizacije.

Da bi si po takem dogodku lahko kar najhitreje opomogli, je nujno vzpostaviti strategijo, s pomočjo katere boste razporedili odgovornosti in sredstva in razumeli tveganja, načrtovali za krizo, oblikovali varnostne mehanizme in strukturirali delovanje. S certifikatom ISO 22301 bo vaša organizacija izboljšala prožnost celotnega poslovnega ekositema in družbe, v kateri deluje. Prav tako boste deležnike pomirili s sporočilom, da lahko prenesete krizo in si od nje hitro opomorete.

Poleg večjega ugleda vam hitro okrevanje po incidentu omogoča, da zmanjšate nevarnosti za lastnino, vas ščiti pred izpadom dohodka in vam pomaga ohraniti likvidnost. S tem zagotovite varnost zaposlenih in zmanjšate tveganje za kršenje zakonodaje.

Za več informacij **kliknite tukaj**.

UPRAVLJANJE PREMOŽENJA: ISO 55001 AMS

Uspešno upravljanje z materialnim in nematerialnim premoženjem vaše organizacije podpira donosnost naložb, hkrati pa vam pomaga, da delujete v skladu s predpisi glede zdravja, varnosti in okolja.

Implementacija sistema vodenja ISO 55001 vam pomaga uravnovesiti tveganja in stroškovno učinkovitost pri sprejemanju odločitev, na primer, ko postavljate prioritete za vzdrževanje premoženja. Prispeva k zniževanju stroškov, povečuje donosnost premoženja in optimizira rasti v celotnem življenjskem ciklu premoženja – vse to bo izboljšalo delovanje in ustvarilo vrednost.

Certifikat ISO 55001 poveča vrednost enega najpomembnejših delov vašega premoženja: vašega ugleda. Certifikat zagotavlja transparentnost uporabe sredstev in odgovorno upravljanje premoženja, kar pošilja močno sporočilo deležnikom in vas ločuje od drugih organizacij. Certifikat prav tako prispeva k povečanju dobičkov, ker vam pomaga prepoznati priložnosti za izboljševanje, v poslovno kulturo vaše organizacije pa trdno zasidra dobro upravljanje premoženja.

Za več informacij **kliknite tukaj**.

Certifikati, osredotočeni na **TVEGANJA, KRITIČNA ZA DELOVANJE**

ANTI-BRIBERY: ISO 37001 ABMS

Za vsako organizacijo je korupcija resna grožnja. Za njeno zatiranje si prizadevajo tudi nedavno sprejete konvencije ZN in OECD. Posledica konvencij so protikorupcijski zakoni, sprejeti v 41 državah.* Organizacije, katerih predstavnike odkrijejo pri dajanju ali prejemanju podkupnin, bodo doletele finančne kazni, direktorji pa tvegajo osebno kazensko in civilno odgovornost.

Izvajanje sistema vodenja, skladnega z ISO 37001, pomeni vzpostavitev postopkov, ki preprečujejo, odkrivajo in obvladujejo tveganje korupcije v vaši organizaciji. Certifikat dokazuje skladnost z zakonodajo in kaže na transparentnost, saj ste svoje delovanje glede protikorupcijskih politik in procesov odprli za pregled tretje strani.

V nekaterih državah je sistem usklajenosti neposredna zakonska zahteva; v drugih je lahko certifikat dokaz, da je organizacija sprejela proaktivne korake, da bi zaposlenim preprečila zapletanje v korupcijo, in kaže, da so kakršni koli prekrški posledica neposlušnosti zaposlenih, in ne pomanjkljive kulture organizacije. Certifikat ISO 37001 deležnikom vaše organizacije in splošni javnosti pošilja jasno sporočilo, spodbuja zaupanje in povečuje vaš ugled.

Za več informacij **kliknite tukaj**.

**Zakonodaja vključuje Zakon o tujih korupcijskih dejanjih (Foreign Corrupt Practices Act ali FCPA) v ZDA in Zakon o podkupovanju (UK Bribery Act) v Združenem kraljestvu iz leta 2010; oba imata mednarodni doseg.*

> *Certifikat dokazuje skladnost z zakonodajo in kaže na transparentnost, saj ste svoje delovanje glede protikorupcijskih politik in procesov odprli za pregled tretje strani.*

VARSTVO PODATKOV: GDPR

Da bi spodbudili zaupanje v vaše obvladovanje podatkov, ni dovolj, da implementirate ustrezne postopke vodenja, nujno je, da pridobite certifikat. Splošna uredba EU o varstvu podatkov (EU GDPR) (ki že velja, zavezujoča pa je od 25. maja 2018 naprej) zaostruje nadzor nad organizacijami, ki upravljajo s podatki državljanov EU, in predpisuje denarne kazni za neskladnost. V odgovor je Bureau Veritas razvil tehnični standard in prostovoljni program certificiranja.

Uvajanje strogih postopkov za ravnanje spodatki omejuje tveganje za potencialno drage kršitve varnosti, varuje zasebnost strank in ščiti dragocene podatke, ki so ključnega pomena za vašo organizacijo. Certificiranje postopkov za varstvo podatkov vam omogoča, da dokažete prizadevanja svoje organizacije za delovanje v skladu s pravili. Če pride do vdora, certifikat tako kaže na potrebno skrbnost in vam lahko pomaga ublažiti potencialne kazni.

Za več informacij **kliknite tukaj**.

Bureau Veritas

USPOSABLJANJE IN CERTIFICIRANJE

Portfelj storitev Bureau Veritas za obvladovanje tveganja podpira podjetja pri zaščiti informacijskih sistemov in fizičnega premoženja in pri proaktivnem obravnavanju nastajajočih poslovnih tveganj.

CERTIFICIRAJE

S svojim odjemalcem certificiranje sistemov vodenja ponujamo že vse od leta 1987, ko je nastal prvi mednarodni standard za sistem vodenja kakovosti, ISO 9001.

Bureau Veritas je akreditiran s strani več kakor 40 nacionalnih in mednarodnih akreditacijskih teles po vsem svetu, hkrati pa je tudi samo pridobilo globalno akreditacijo United Kingdom Accreditation Service (UKAS) za standarde ISO 27001, ISO 55001 in ISO 22301, ISO9001, ISO14001, ISO45001 in zaprosilo za ISO 37001.

USPOSABLJANJE

Bureau Veritas nudi tudi usposabljanja, ki vam pomagajo razumeti standarde in kako jih uporabiti v vaši organizaciji. Naša usposabljanja izvajajo vodilni presojevalci z večletnimi izkušnjami in razumevanjem industrije; usposobljeni so za medosebno komunikacijo, medkulturna vprašanja in koncepte poučevanja odraslih.

UČENJE V RAZREDU

Nudimo enodnevne uvodne seminarje za vsak standard, dvodnevne izpopolnjevalne tečaje za poglobljene informacije, dvodnevni tečaj za notranje presojevalce in petdnevnega za vodilne presojevalce.

E-UČENJE

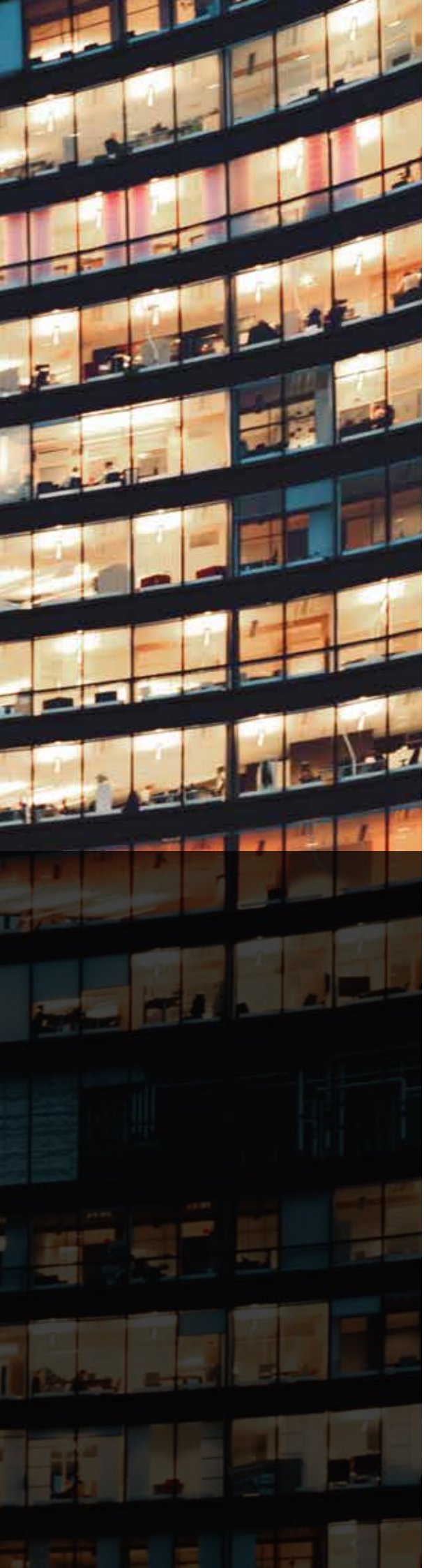
Nedavni dodatek k naši ponudbi usposabljanja, moduli za eUčenje, vključujejo trening ozaveščanja in specifične module o tem, kako aplicirati metodologije analize tveganj ali kontekst organizacije glede na specifična področja tveganj.

KOMBINIRANO UČENJE

Paketi kombiniranega učenja vsebujejo komponente iz različnih seminarjev, ustrezni moduli eUčenja pa pomagajo udeležencem osvežiti in posodobiti znanje, ki so ga najprej pridobili v razredu.

Prosimo, upoštevajte, da vsa izobraževanja niso na voljo v vseh državah. Spletna stran Bureau Veritas za vašo državo ima več podrobnosti o klasičnih tečajih, ki so na voljo lokalno.

Za več podrobnosti o našem portfelju podjetniškega tveganja obiščite naše strani operativnega tveganja.



O BUREAU VERITAS

Bureau Veritas Certification: vodilna certifikacijska hiša v Sloveniji in na svetu

Bureau Veritas Certification nudi obširen portfelj storitev certificiranja na področju kakovosti, okolja, varnosti in zdravja, informacijske varnosti, energije ter družbene odgovornosti po mednarodno priznanih standardih, lokalnih shemah in rešitvah prilagojenih potrebam strank.

Podeljenih je bilo več kot 100.000 certifikatov v 100 državah po vsem svetu. Pridobljena certifikacijska oznaka Bureau Veritas pomeni pomembno konkurenčno prednost in sporoča zavezanost vaše organizacije k odličnosti, zanesljivosti in trajnostnemu razvoju.

Za več informacij se obrnite na:

Bureau Veritas, d.o.o.
Linhartova cesta 49a
1000 LJUBLJANA

Tel.: + 386 1 47 57 600

www.bureauveritas.si

Obiščite naše spletne stani
Operativno tveganje

Oblikovanje in izdelava: BOLDcie.com
Foto: Bureau Veritas / iStock / Thinkstock