

Novosti pri pravilih notranjega revidiranja

Tina Toman Pfajfar



Gradivo je last Slovenskega inštituta za revizijo in je predmet avtorske zaščite in drugih oblik zaščite intelektualne lastnine. Prepovedano je kakršnokoli reproduciranje, razen izključno za osebno uporabo in v nekomercialne namene, pri čemer se morajo ohraniti vsa opozorila o avtorskih ali drugih pravicah, zato se ne smejo prepisovati, razmnoževati ali kako drugače razširjati. Naveden mora biti tudi vir.

2.3. Sodelovanje med notranjimi revizorji temelji na tovarištvu, odkritosti in izmenjavanju izkušenj. Notranji revizor svojemu stanovskemu tovarišu ne odreče pomoči v obliki nasveta ali mnenja. **Ceni in spoštuje znanje, dostojanstvo in strokovnost vsakega sodelavca** v notranjerevizijski dejavnosti in drugih dejavnostih.

Od notranjega revizorja se pričakuje, da je sposoben prepoznavati in predvidevati tveganja, ločevati bistveno od nebistvenega, spodbujati in navduševati zaposlene v organizaciji za uvajanje sprememb in člane revizijske skupine za uspešno opravljanje notranjerevizijskih nalog, dojemati razumno poslovno sebičnost znotraj sprejemljivih in sprejetih moralnih norm ter da je **človek s strokovno in moralno širino, ki se kaže v njegovi poštenosti in pravičnosti**, iniciativnosti, motiviranosti, odgovornosti, molčečnosti, lojalnosti, zanesljivosti, neodvisnosti, nepristranskosti, resnicoljubnosti, vestnosti, prizadevnosti, iznajdljivosti, natančnosti, odkritosti, pripravljenosti strokovno pomagati sodelavcem, ukaželnosti, radovednosti, ustvarjalnosti.

- Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju
- GTAG Revidiranje upravljanja omrežij in omrežno komuniciranje
- COSO Navodilo za upravljanje tveganj prevar
- COSO Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju
- ZJF
- Drugo

Mednarodni standardi strokovnega ravnanja pri notranjem revidiranju

- International Internal Audit Standards Board completes review of public comments on Global Internal Audit Standards (theiia.org) (31. 10. 2023)

The most frequently recurring comments of concern included:

- An increased usage of the word “must,” making the Standards seem too prescriptive.
- Unclear requirements for external quality assessments.
- The applicability of the Standards to public sector and small internal audit functions.
- Missing or vague terminology in the Purpose of Internal Auditing.
- Requirements for 20 hours of continuing professional education and specific competencies for all internal auditors.
- Requirements for board actions stated too directly and missing responsibilities for senior management.
- Unclear distinction between internal audit mandate and the internal audit charter.
- Confusion about appropriate measures of internal audit performance.
- The applicability of requirements to both assurance engagements and advisory engagements.
- Requirement for internal auditors to make recommendations related to findings.
- Perceived requirement of “ratings” and “rankings” for findings and conclusions.
- Requirement for a statement of conformance or nonconformance in final engagement communications.

Temeljna načela strokovnega ravnanja pri notranjem revidiranju

Notranji revizor:

1. izkazuje neoporečnost,
2. izkazuje strokovnost in potrebno poklicno skrbnost,
3. je nepristranski in brez nedopustnega vplivanja (neodvisen),

Notranja revizija:

4. je usklajena s strategijami, cilji in tveganji organizacije,
5. ima primerno mesto v organizaciji in ustrezne vire,
6. izkazuje kakovost in nenehno izboljševanje,
7. učinkovito komunicira,

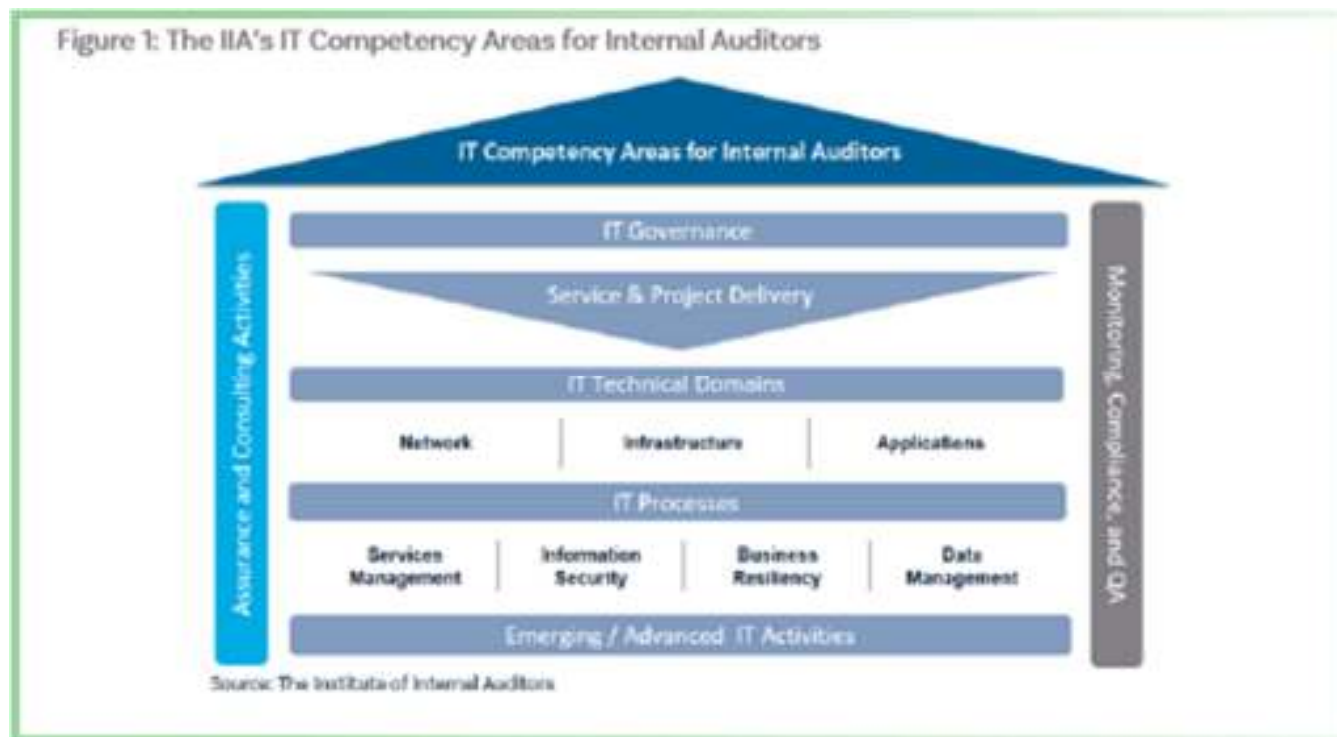
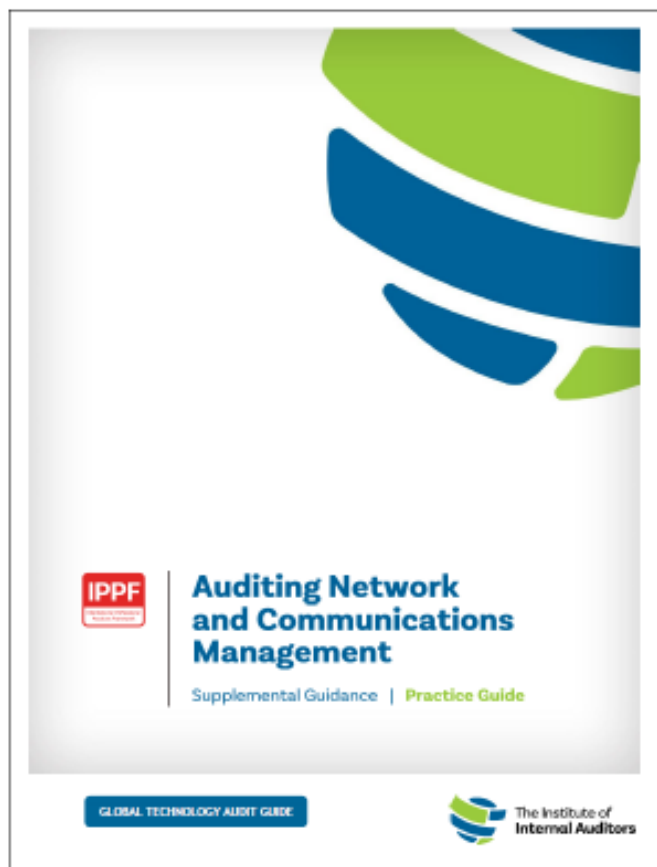
Rezultati dela:

8. dajejo zagotovila na podlagi ocene tveganj,
9. izkazujejo prodornost, proaktivnost in usmerjenost v prihodnost,
10. spodbujajo izboljšave v organizaciji.

VS.



Revidiranje upravljanja omrežij in omrežno komuniciranje



Revidiranje upravljanja omrežij in omrežno komuniciranje

- zagotoviti, da so cilji, tveganja in notranje kontrole omrežij in omrežnega komuniciranja povezani s strategijo in cilji organizacije; zahteve, pričakovanja in viri morajo biti konkretizirani v politikah, postopkih in finančnih ter tehničnih planih
- upravljanje domen (vzpostavljen popis obstoječega stanja)
- vzpostavljeno upravljanje omrežnega komuniciranja (izmenjava podatkov, uporaba oblačnih storitev)
- dostopi do omrežja so zagotovljeni le za pooblaščne račune, urejen proces spremljanja dostopov in način dostopanja do zunanjih omrežij
- redno spremljanje dogodkov; skupaj z odgovornimi za kibernetško varnost se analizirajo vse »neobičajne« aktivnosti

Revidiranje upravljanja omrežij in omrežno komuniciranje

- kontrole dostopa
- kibernetska varnost
- oddaljeni dostopi
- Revidiranje odzivanja in okrevanja po kibernetskem incidentu
- Revidiranje delovanja kibernetske varnosti: preprečevanje in odkrivanje
- Revidiranje mobilnega računalništva
- Tveganja??

Revidiranje upravljanja omrežij in omrežno komuniciranje

- COBIT 2019 vsebuje 40 ciljev, ki so razdeljeni na 1202 aktivnosti
- NIST 800-53, 298 kontrol in 709 podkontrol
- CIS Controls Verison 8, ki vsebuje 18 kontrol

- *COBIT 2019 Framework: Governance and Management Objectives practices:*

- BAI09.02 Manage Critical Assets.
- DSS05.02 Manage Network and Connectivity Security.
- DSS05.03 Manage Endpoint Security.

- *NIST SP 800-53r5 controls:*

- AC-17 Remote Access.
- AC-19 Access Control for Mobile Devices.
- AC-20 Use of External Systems.
- AU-16 Cross-Organizational Audit Logging.
- CA-3 Information Exchange.
- SC-7 Boundary Protection.

- *CIS Controls safeguards:*

- 12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure.
- 13.5 Manage Access Control for Remote Assets.

Navodilo za upravljanje tveganj prevar

- druga izdaja, marec 2023
- zadnja dognanja na področju preprečevanja prevar
- posodobljena terminologija
- obravnava tudi razvoj tehnologije in analizo podatkov
- namenjen organizacijam vseh velikosti in vsem industrijam, pri čemer je jasno zapisano, da mora biti prilagojen kompleksnosti, področju dela in drugim dejavnikom

Navodilo za upravljanje tveganj prevar

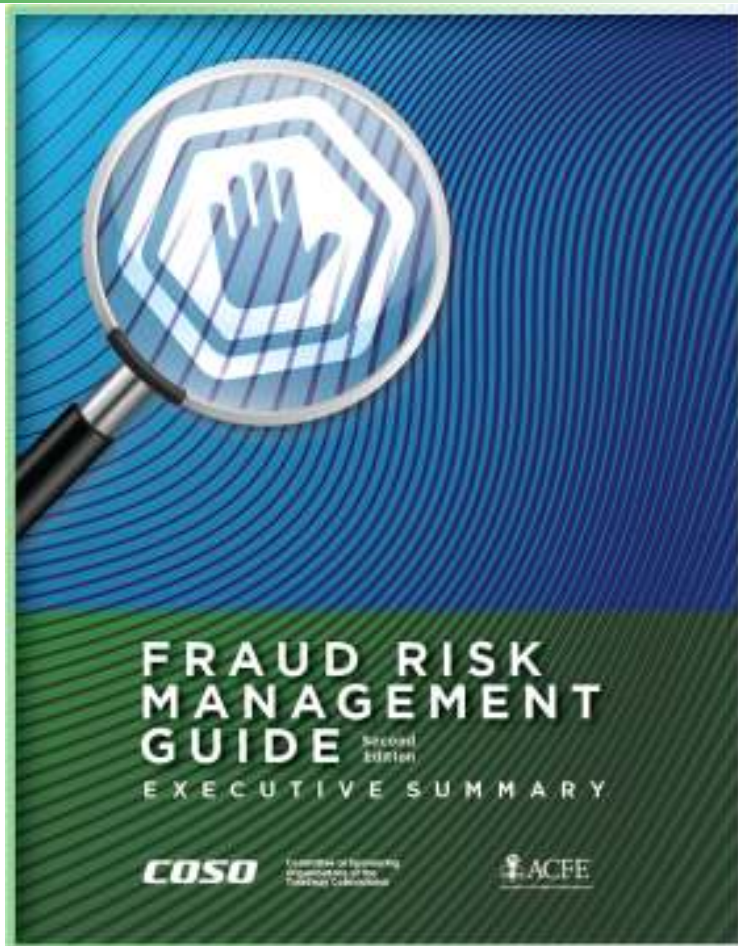


Figure 1. Ongoing, Comprehensive Fraud Risk Management Process



Navodilo za upravljanje tveganj prevar

PG Notranja revizija in prevare

Dokument ponuja dve možnosti za implementacijo programa preprečevanja prevar:

- uporabo drugega načela iz dokumenta (izvedba celovite presoje tveganj za prepoznavo shem prevar in tveganj, povezanih z njimi, ocenjevanje verjetnosti in pomembnosti, presoja obstoječih aktivnosti in priprava akcijskih načrtov izboljšanja obvladovanja tveganj, če je to potrebno), pri čemer organizacija upošteva osmo načelo iz Celovitega okvira notranjega kontroliranja (Organizacija prouči možnosti za prevare pri ocenjevanju tveganj za doseganje ciljev), ali
- v celoti implementira vsebino prenovljenega navodila, ki vsebuje pet načel za preprečevanje prevar.

Relationship Between the COSO 2013 IC Framework's Five Components and 17 Internal Control Principles and this Guide's Five Fraud Risk Management Principles

COSO revised its *Internal Control — Integrated Framework* in 2013 to incorporate 17 principles. These 17 principles are associated with the five internal control components COSO established in 1992. This Guide's five fraud risk management principles fully support, are entirely consistent with, and parallel the COSO 2013 IC Framework's 17 internal control principles. The correlation between the fraud risk management principles and the COSO 2013 IC Framework's internal control components and principles is as follows:

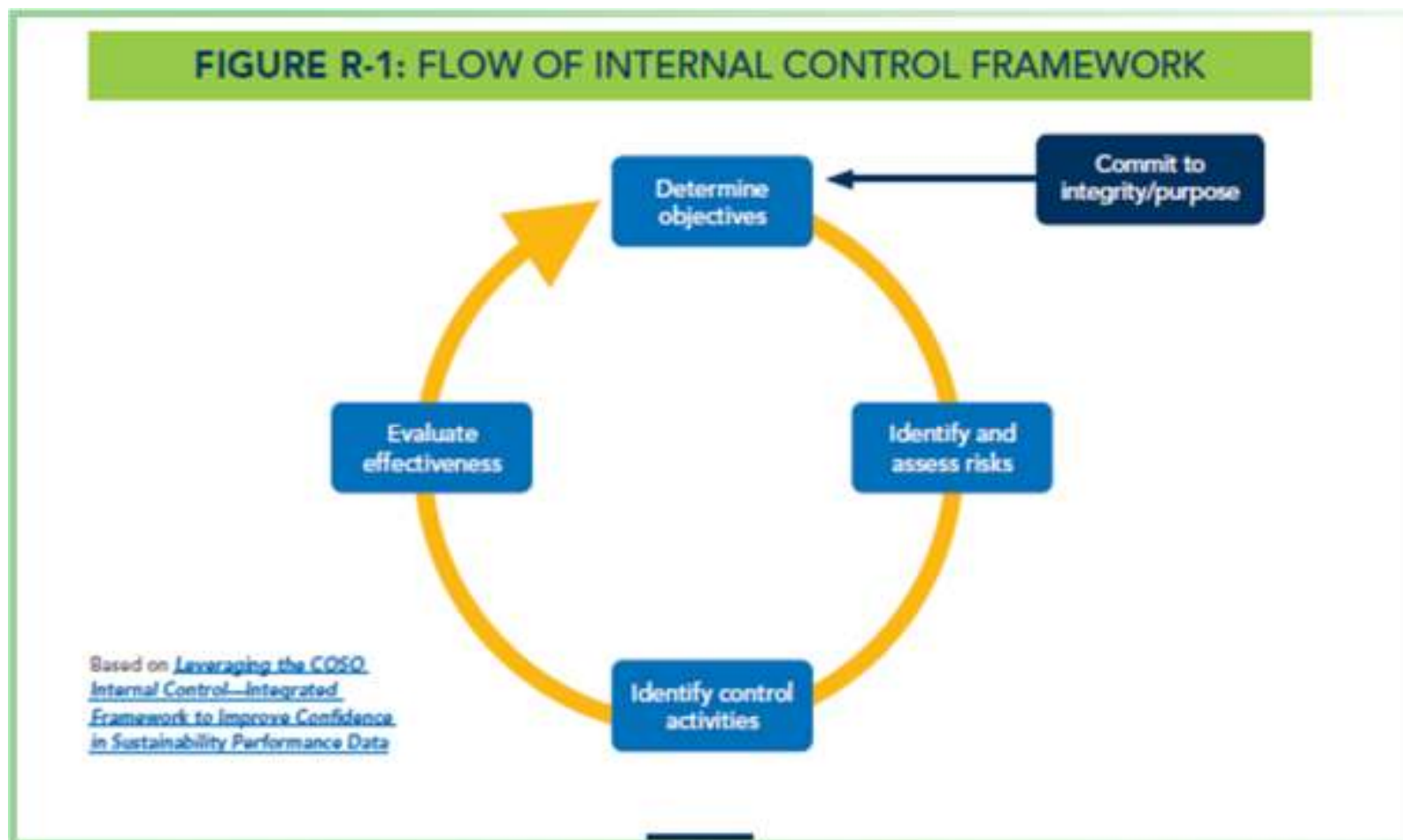


Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju

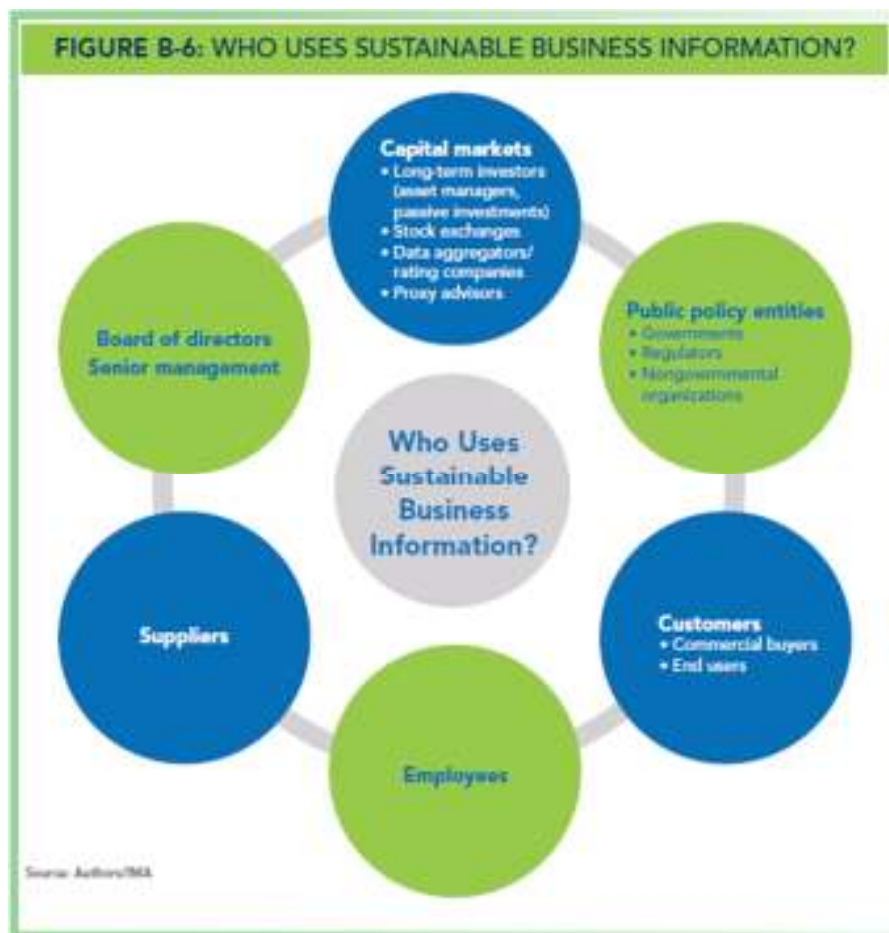
- opredelitve najpomembnejših pojmov
- 17 načel Celovitega okvira notranjega kontroliranja v povezavi s trajnostnim poročanjem
- pri vsakem načelu so npr. dodatno izpostavljene zaveze, da organizacija spoštuje tudi vsa pričakovanja, povezana z upravljanjem okoljskih, družbenih in upravljavskih tveganj



Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju



Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju



Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju

TABLE B-1: ESG TOPICS

Environmental	Social	Governance
Biodiversity	Community relations	Anti-bribery and anti-corruption
Climate change	Data privacy	Anti-fraud
Deforestation	Diversity, equity, and inclusion	Corporate board, structure
Energy use	Education and training	Data protection
Extreme weather	Employee compensation and benefits	Executive compensation policies
GHG emissions	Employee engagement	Regulatory compliance
Landfill	Health and safety, product use	Shareholder rights and engagement
Oceans	Health and safety, production	Transparency, disclosure
Recycling	Human rights	Whistleblower policy
Soil health	Modern slavery	
Transportation	Opportunities for meaningful work	
Water management	Union rights	

Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju

- Pomoč pri določanju odgovornosti
 - Tudi razumevanje koncepta NK
- Kako sta vizija/poslanstvo povezana s cilji
- Sodelovanje (multidisciplinarnost)
- Kako si lahko pomagamo z obstoječim sistemom za finančno poročanje
- Kako preoblikovati obstoječe kontrole
- Bistvena je materialnost
- Začnimo zdaj 😊

Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju

FIGURE B-4: COMPONENTS, PRINCIPLES, AND POINTS OF FOCUS

Components	Principles	No. of Points of Focus
<div> <div>Central Environment</div> <div>Risk Assessment</div> <div>Control Activities</div> <div>Information & Communication</div> <div>Monitoring Activities</div> </div>	1. Commitment to integrity and ethical values	4
	2. Independent board of directors oversight	4
	3. Structures, reporting lines, authorities, responsibilities	3
	4. Attract, develop, and retain competent people	4
	5. People held accountable for internal control	5
	6. Clear objectives specified	15
	7. Risks identified to achievement of objectives	5
	8. Potential for fraud considered	4
	9. Significant changes identified and assessed	3
	10. Control activities selected and developed	6
	11. General IT controls selected and developed	4
	12. Controls deployed through policies and procedures	6
	13. Quality information obtained, generated, and used	5
	14. Internal control information internally communicated	4
	15. Internal control information externally communicated	5
	16. Ongoing and/or separate evaluations conducted	7
	17. Internal control deficiencies evaluated and communicated	3

Source: [Probita](#)

POINTS OF FOCUS

► Sets the tone at the top

An organization's actors look to how senior leadership behaves, speaks, acts, and directs others to act.⁴ Senior leadership can prioritize and facilitate the building of respect toward building a sustainable business. Senior leaders can influence conduct and performance by behaving as role models.

► Establishes standards of conduct

Organizations establish standards of conduct for their actors. Often, an organization, at its highest levels, operationalizes its mission or purpose through a values statement. These values are then further operationalized with sustainable business programs and policies that are communicated throughout the organization.

► Evaluates adherence to standards of conduct

Organizations establish a system or processes to assess whether its actors are complying with its established values and policies, including those that apply to values and policies that support the organization's efforts to act sustainably. This means developing oversight processes, including internal audit review, if appropriate.

► Addresses deviations in a timely manner

An organization follows up when an actor (or group) diverges from its policies around sustainable business management and reporting. This is effectuated through communications and follow-up with the purpose of correcting course and supporting improvement and development.

Doseganje uspešnega sistema notranjih kontrol pri trajnostnem poročanju

CEO LETTERS

A widespread practice in setting the tone at the top and setting sustainable business priorities is the CEO letter. For example, in its [2021 sustainability report](#), United States Steel President and CEO David B. Burritt states:

Steel is critical to a healthy manufacturing base, and it is incumbent upon companies like ours to take the necessary steps to remain economic engines that best support their employees, best serve their customers, best enrich their communities, and best reward their stockholders. We believe the key to achieving all of these things is making sustainability central to who we are and what we do....our Best for All approach to sustainability...is making it possible for us to get to our future faster—a future where we are leading our industry in the development of innovative, profitable, and sustainable steel solutions that are best for people and the planet.

Moving to put the message into practice, Burritt and the company's board of directors appointed a new chief strategy and sustainability officer, who has joined the senior management team. This sends a message that sustainability is core to the company achieving its long-term strategy to further its mission.

CEO ANNOUNCEMENT: B CORP

In March 2022, [The Vita Coco Company](#) announced that it had become a Certified B Corporation. In the announcement, Mike Kirban, founder and co-CEO, stated:

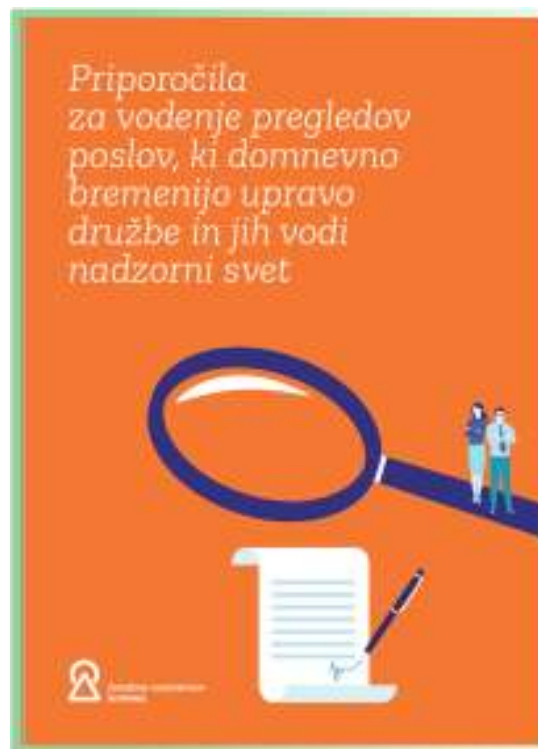
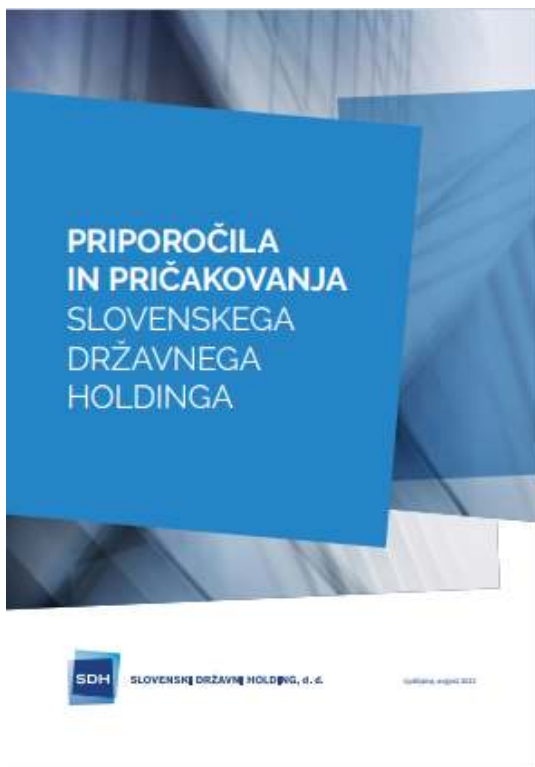
We've always been on a mission to create more equitable access to natural, better-for-you products in a responsible way. Joining a network of like-minded organizations will create collective impact to democratize health and wellness. We are honored to receive this distinction and become part of the B Corp community.

This is indeed a control activity, because it announces to all stakeholders the company's commitment to its mission. From this, the company engages all stakeholders to contribute resources to reach its objectives, which include positive impact on farming communities in the Philippines, Sri Lanka, and Ecuador.

100.b člen

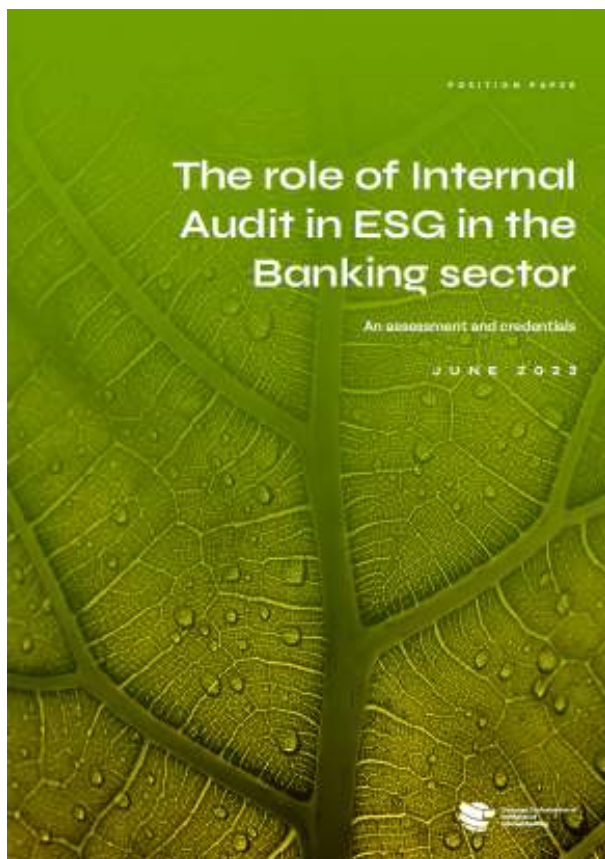
(Register zunanjih izvajalcev, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov)

- (1) Zunanji izvajalci, pooblaščenih za notranje revidiranje, lahko izvajajo notranje revidiranje neposrednih in posrednih uporabnikov, če:
- zagotovijo, da za njih notranje revidiranje pri neposrednih in posrednih uporabnikih v skladu s četrtem, petim in šestim odstavkom 100. člena tega zakona izvajajo notranji revizorji z nazivom državni notranji revizor ali preizkušeni državni notranji revizor, in
 - so vpisani v register zunanjih izvajalcev, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov, ki ga vodi urad, pristojen za nadzor proračuna.
- (2) V register zunanjih izvajalcev, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov, se na podlagi vloge vpiše pravna oseba zasebnega prava ali samostojni podjetnik posameznik, če:
- razpolaga z notranjimi revizorji z nazivom državni notranji revizor ali preizkušeni državni notranji revizor, ki zanj v skladu s četrtem, petim in šestim odstavkom 100. člena tega zakona izvajajo notranje revidiranje neposrednih in posrednih uporabnikov,
 - oseba, pooblaščenega za zastopanje zunanjega izvajalca, pooblaščenega za notranje revidiranje neposrednih in posrednih uporabnikov, ni bila pravnomočno obsojena za kaznivo dejanje zoper premoženje oziroma gospodarstvo.
- (3) Notranji revizorji iz prve alineje prejšnjega odstavka so pri zunanjih izvajalcih, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov, zaposleni ali zanje na podlagi pogodbe izvajajo storitve notranjega revidiranja neposrednih in posrednih uporabnikov.
- (4) Za namen vodenja registra zunanji izvajalci, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov, zagotavljajo naslednje podatke:
- ime subjekta, sedež, matično številko in pravno obliko,
 - osebno ime osebe, pooblaščenega za zastopanje,
 - kontaktne podatke.
- (5) Vsako spremembo podatkov iz drugega in četrtega odstavka tega člena zunanji izvajalci, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov, sporočijo uradu, pristojnemu za nadzor proračuna, najkasneje v osmih dneh po nastanku spremembe.
- (6) Register zunanjih izvajalcev, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov, vsebuje registracijsko številko in podatke iz četrtega odstavka tega člena ter je javen. Objavljen je na spletni strani urada, pristojnega za nadzor proračuna.
- (7) Zunanjega izvajalca, pooblaščenega za notranje revidiranje neposrednih in posrednih uporabnikov, urad, pristojen za nadzor proračuna, izbriše iz registra, če:
- sam pisno zahteva izbris;
 - je bil izbrisan iz sodnega registra;
 - je bila oseba, pooblaščenega za zastopanje zunanjega izvajalca, pooblaščenega za notranje revidiranje neposrednih in posrednih uporabnikov, pravnomočno obsojena za kaznivo dejanje zoper premoženje oziroma gospodarstvo;
 - ne izpolnjuje pogojev iz prve alineje prvega odstavka in iz prve alineje drugega odstavka tega člena.
- (8) V primeru, da urad, pristojen za nadzor proračuna, zunanjega izvajalca, pooblaščenega za notranje revidiranje neposrednih in posrednih uporabnikov, izbriše iz registra zaradi neizpolnjevanja pogojev iz drugega odstavka tega člena, lahko zunanji izvajalec ponovno poda vlogo za vpis v register, ko zagotovi izpolnjevanje teh pogojev.
- (9) V primeru, da urad, pristojen za nadzor proračuna, zunanjega izvajalca, pooblaščenega za notranje revidiranje neposrednih in posrednih uporabnikov, izbriše iz registra, ker ugotovi, da pri posameznem neposrednem ali posrednem uporabniku:
- ni zagotovil, da notranje revidiranje zanj izvajajo notranji revizorji z nazivom državni notranji revizor ali preizkušeni državni notranji revizor, ali
 - notranji revizorji z nazivom državni notranji revizor ali preizkušeni državni notranji revizor, s katerimi razpolaga zunanji izvajalec, pooblaščen za notranje revidiranje neposrednih in posrednih uporabnikov, ne izvajajo notranjega revidiranja neposrednih in posrednih uporabnikov v skladu s četrtem, petim in šestim odstavkom 100. člena tega zakona,
- lahko zunanji izvajalec poda vlogo za ponovni vpis v register po preteku enega leta od dneva izbrisa iz registra.
- (10) Minister, pristojen za finance, predpiše vsebino in obliko vloge, dokazila o izpolnjevanju pogojev za vpis ter vsebino in obliko obvestila o spremembah podatkov v registru zunanjih izvajalcev, pooblaščenih za notranje revidiranje neposrednih in posrednih uporabnikov.



Namen tega dokumenta je članom nadzornih svetov in članom komisij nadzornega sveta, ki jim je bila naloga dodeljena, predstaviti priporočila in izkušnje glede vodenja pregledov poslov, ki so domnevno škodljivi za družbo in bremenijo upravo družbe. Ti postopki se pogosto začnejo z anonimnimi pismi z opisi očitkov glede domnevnih nepravilnosti uprave.

večletno poslovanje družbe in skupin, redno poročanje, nabava blaga in storitev, sponzorstvo in donatorstvo, optimizacija stroškov, upravljanje korporativne kulture, trajnostno poslovanje, upravljanje tveganj



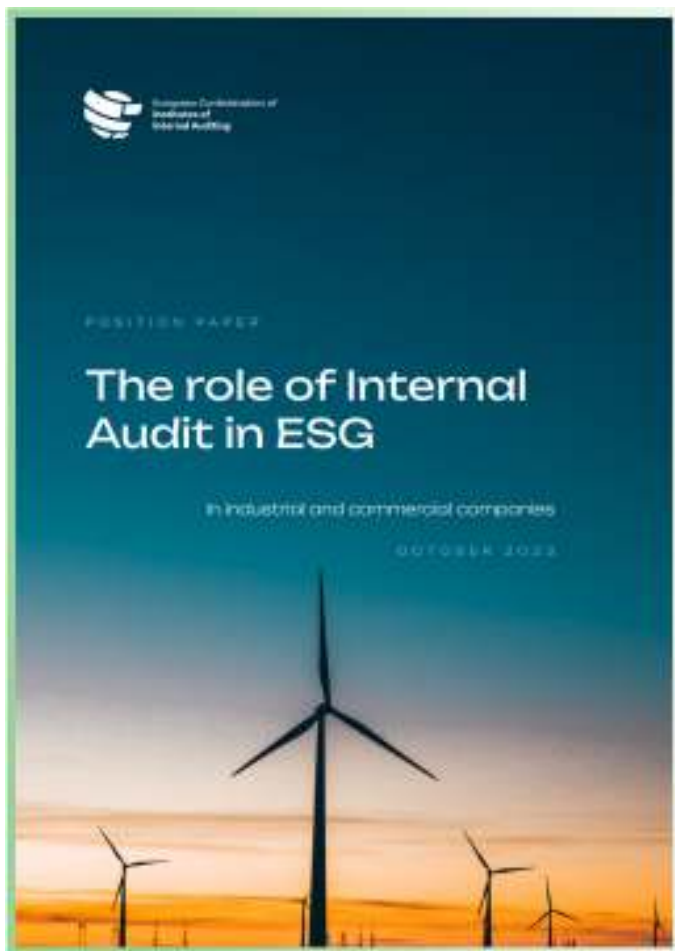
Internal vs External Audit on ESG

While the internal and external audit functions could complement each other, their purposes and areas of focus differ. The Institute of Internal Auditors (IIA) emphasizes that the two functions do not compete or conflict; rather, they both contribute to effective governance. In general, internal auditors take a holistic view of their organization's governance, risk, and control systems (in other words, primarily non-financial information), while external auditors are either concerned with the accuracy of business accounts and the organization's financial condition and its regulatory compliance.

With regard to ESG, Internal Audit can provide the independent internal assurance needed for trustworthy ESG disclosures and help to ensure the existence and effectiveness of internal controls on ESG risks and their continuous monitoring processes across the organization. External auditors provide third-party assurance services by endorsing the integrity of non-financial (ESG-related) public disclosures and ensuring they align with financial information in external reporting to investors and stakeholders. External auditors can also help to perform a benchmark to compare the entity with competitors and ESG best practices in the financial sector.

While the purpose, focus, and outcomes of their fieldwork may vary, internal and external auditors often share information to avoid duplication and improve audit coverage. In fact, Internal Audit can leverage the external auditor's comments / findings on areas included in their review and vice versa.

ESG - ECIIA



ADVICE / INSIGHT

Give input on ESG management control cycle

Give input on ESG embedding progress

Give input on ESG reporting process
including double materiality assessment

Give input on ESG governance

Give input on ESG culture

Give input on ESG strategy

ASSURANCE

Audit effectiveness ESG governance

Audit effectiveness risk management

Audit design and effectiveness ESG processes
including double materiality assessment

Audit ESG management control cycle

Review strategic changes

Assess ESG data collection

Coordinate Assurance with 2nd line

Provide int. assurance on ESG reporting process

NOT FOR INTERNAL AUDIT

Define ESG risks & opportunities

Define ESG strategy & business transformation

Manage ESG risk & opportunities

Play the role of external assurance provider

Adapt internal controls & define KPIs

Change culture

Accountability on ESG goals & achievements

workiva

The ESG Checklist for Internal Audit:


Guide to Regulations, Risks, and Roles

As organizations embark on their ESG journey, the role of internal audit and risk professionals is becoming increasingly visible and critical to help drive ESG performance. From assessing a broad range of ESG-related risks to ensuring the completeness and accuracy of sustainability data, ESG presents a unique opportunity for audit professionals to add value and elevate their role as a strategic advisor.

But with an ever-changing ESG landscape, how can internal auditors take advantage of this opportunity to help their organizations prepare?

This checklist can help. Use it as a starting point to identify key actions. We'll review items for identifying and assessing ESG-related risks, what to consider and how

to set up processes to comply with global regulations, and what roles your team and other departments can take to drive ESG program success. And to note, your ESG program is an ongoing effort that will require continuous evaluation—from the internal controls you establish to the people you involve, internal audit teams need to remain agile. With that in mind, let's dive in!

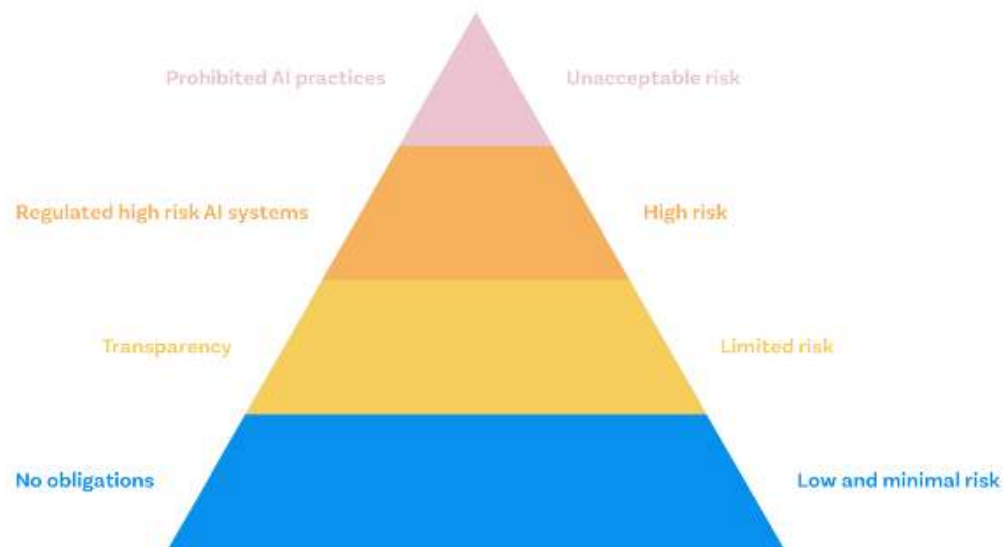


Given the importance, here's a checklist to help you get started:

- Engage key stakeholders, including the board of directors, to discuss how your organization is approaching ESG
- Conduct a **materiality assessment** and create a list of the topics that are material to your organization
- Understand how ESG aligns with your organization's strategy and pinpoint the ESG topics that are most applicable to your business
- Familiarize yourself with your organization's current ESG program and what's being reported both internally or externally
- Integrate material ESG-related risks into your broader enterprise risk assessment and management process
- Start auditing the completeness and accuracy of any current ESG-related metrics that your organization reports externally
- Develop, implement, and harmonize policies, processes, controls, and control activities to maximize ESG opportunities and mitigate risks
- Implement monitoring activities across the second and third lines of defense to determine if control activities are yielding expected results and helping achieve ESG commitments
- Establish a regular reporting process to share relevant information with stakeholders on ESG performance and compliance with regulatory requirements
- Re-evaluate and respond to new ESG-related risks with appropriate internal controls
- Schedule retrospective reviews to determine what's working well and how to continuously improve



Figure 8. Risk-based approach in AI (subject to changes) (EPRS, 2022)



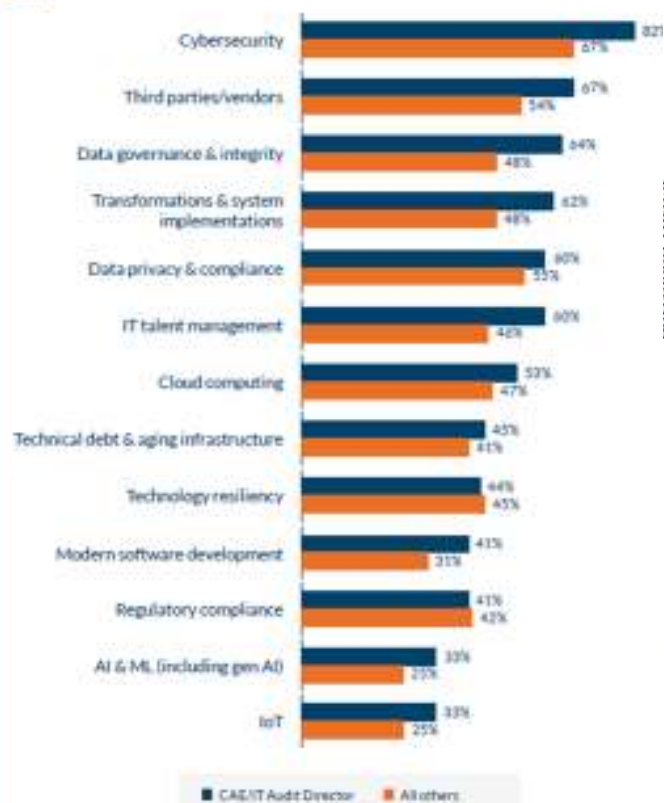


Our key findings

- Cybersecurity is the top priority ... and by a wide margin.
- AI is an emerging risk with gaps in organisational preparedness and audit proficiency.
- The talent gap in IT is a growing concern.
- Data privacy is a growing regulatory challenge.
- Data governance and transformation are of significant concern.
- Navigating the complex landscape of third-party and vendor risk is a challenge.
- More frequent auditing drives risk preparedness.

Perceived threat of technology risks in next 12 months (CAEs/IT Audit Directors vs. all others)

Figure 2

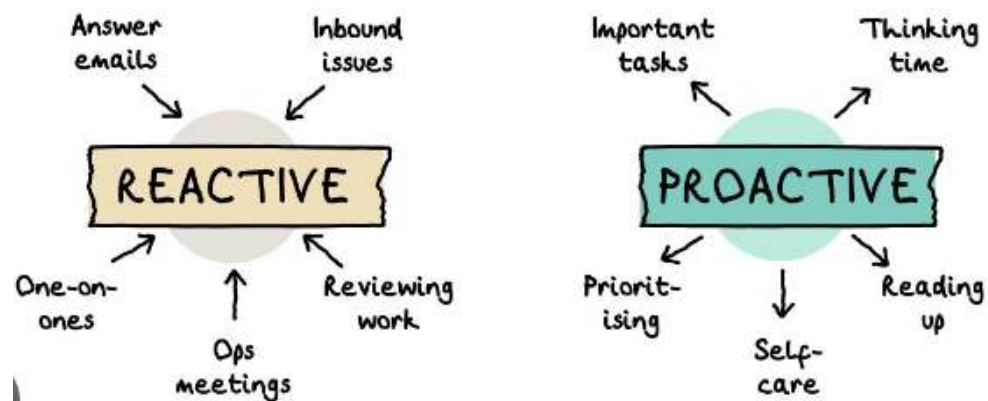


Hvala za pozornost!



Zmota # 3: Vse zmorem sam.

Reactive vs. Proactive Time



<https://www.dave-bailey.com/blog/proactive-vs-reactive>