Dokument i UDHËZUES GAP sipas Standartit ISO 27001:2022

Ky dokument ofron një përmbledhje të ndryshimeve kryesore midis versionit 2013 dhe 2022 të ISO 27001. Kërkesat e reja tregohen më poshtë. Do t'ju duhet të përgatiteni për ndryshim dhe të përshtatni sistemin tuaj të menaxhimit të sigurisë së informacionit për të përmbushur kërkesat e reja dhe afatet kohore kalimtare. Ky dokument duhet të përdoret së bashku me mjetin e analizës së mangësive të AQSCERTsë.

Struktura e ISO 27001:2022 ndjek strukturën e nivelit të lartë të përcaktuar në Aneksin SL:

1- Fushëveprimi;
2- Referencat normative;
3- Termat dhe përkufizimet;
4- Konteksti i kompanisë;
5- Udhëheqja;
6- Planifikimi;
7- Mbështetja;
8- Operacioni;
9- Vlerësimi i performancës;
10- Përmirësimi.

Shtojca A
STRUKTURA E ISO 27001:2022
VLERAT TONA
5. Kontrollet kompaniive
6. Kontrollet e njerëzve

7. Kontrollet fizike

8. Kontrollet teknologjike

KLAUZOLA		KERKESA	MANGESIA
4	Konteksti i kompaniës		
4.2	Kuptimi i nevojave dhe pritshmërive të palëve të interesuara	Ky kontroll tani kërkon në mënyrë të qartë që kompania juaj të jetë në gjendje të demonstrojë se cilat nga kërkesat përkatëse të palëve tuaja të interesuara do të adresohen përmes ISMS.	
4.4	Sistemi I Menaxhimit të Sigurisë së Informacionit (ISMS)	Tani ka një fokus në proceset tuaja dhe mënyrën se si ato ndërveprojnë me ISMS.	
5	Udhëheqja		
5.3	Rolet, përgjegjësitë dhe autoritetet kompaniive	Kjo klauzolë tani përmban një kërkesë të qartë për të komunikuar rolet, përgjegjësitë dhe autoritetet brenda kompaniës suaj.	
6	Planifikimi		
6.2.d	Objektivat e sigurisë së informacionit dhe planifikimi për t'i arritur ato	Objektivat e sigurisë së informacionit duhet të vendosen në nivelet përkatëse brenda kompaniës suaj. ISO 27001:2022 kërkon që objektivat dhe progresi drejt arritjes së tyre të monitorohen.	
6.3	Planifikimi I ndryshimeve	Kjo është një kërkesë e re. Jini të përgatitur për të demonstruar se si planifikoni ndonjë ndryshim në ISMS.	
9	Vlerësimi I performancës		
9.3.2.c	Të dhënat e rishikimit të menaxhmentit	Gjatë rishikimit të menaxhimit, tani pritet që ju të rishikoni çdo ndryshim në nevojat dhe pritshmëritë e palëve tuaja të interesuara.	

ANEKSI A

KLAUZOLA	KERKESA	MANGESIA
5 Kontrollet kompaniive		

5.7	Inteligjenca e kërcënimit	Një kontroll krejtësisht i ri i cili kërkon që kompanitë të mbledhin informacion në lidhje me kërcënimet e sigurisë së informacionit dhe të analizojnë këtë informacion në mënyrë që të prodhojnë inteligjencë kërcënimi. Kompanitë mund të dëshirojnë të marrin në konsideratë se nga do të mbledhin informacion dhe si përcaktojnë se informacioni është i rëndësishëm për nevojat e tyre.
5.23	Siguria e informacionit për përdorimin e shërbimeve cloud	Ky është një kontroll i ri që kërkon që kompanitë të kenë procese të vendosura në mënyrë që të sigurohen që ato të kenë specifikuar, menaxhuar dhe administruar konceptet e sigurisë pasi ato lidhen me shërbimet cloud që kanë vendosur. Ju gjithashtu duhet të merrni parasysh çështjet e sigurisë kur planifikoni daljen tuaj nga shërbimet cloud.
5.3	Gatishmëria e TIK për vazhdimësinë e biznesit	Ky kontroll kërkon që ju të identifikoni kërkesat e vazhdimësisë së TIKut në një situatë të vazhdimësisë së biznesit. Nga ju pritet të tregoni prova objektive se gatishmëria për TIK është integruar plotësisht në planin tuaj të vazhdimësisë së biznesit, duke përfshirë testimin e gatishmërisë për TIK.
7	Kontrollet fizike	
7.4	Monitorimi i sigurisë fizike	Megjithëse kontrollet e sigurisë fizike nuk janë një koncept i ri, standardi tani prezanton kërkesën për të monitoruar ambientet tuaja në mënyrë të vazhdueshme (brenda dhe jashtë orarit normal të punës) për akses fizik të paautorizuar.
8	Kontrollet teknologjike	
8.9	Menaxhimi I konfigurimit	Menaxhimi i konfigurimit të rrjeteve dhe sistemeve tani duhet të krijohet, zbatohet, monitorohet dhe rishikohet. Kjo do të përfshijë identifikimin e kërcënimeve, dobësive dhe dobësive ndaj konfigurimeve të sigurisë.
8.10	Fshirja e informacionit	Ky kontroll kërkon informacion që nuk kërkohet më të fshihet në mënyrë të sigurt kur është i vjetëruar ose nuk kërkohet më.
8.11	Maskimii të dhënave	Një kërkesë e re që të dhënat e ndjeshme të mbrohen duke përdorur teknika mbi dhe përtej kontrolleve dhe protokolleve të rregullta të sigurisë të një kompanie. Informacioni që do të maskohet mund të jetë për shkak të një kërkese ligjore, statutore, kontraktuale ose rregullatore
8.12	Parandalimi i rrjedhjes së të dhënave	Ky kontroll i ri kërkon zbatimin e masave për parandalimin e rrjedhjes së të dhënave për të parandaluar/zbuluar aksesin, transferimin ose nxjerrjen e informacionit të paautorizuar.

8.16	Aktivitetet e monitorimit	Ky kontroll është një zgjerim i 'ISO 27001:2013 A.12.4 Regjistrimi dhe monitorimi'. Në këtë botim të fundit, kompaniave u kërkohet të monitorojnë rrjetet dhe sistemet për sjellje anormale, duke kuptuar se si duket sjellja/përdorimi 'normal'. Ekziston gjithashtu një kërkesë për të treguar se si reagoni ndaj incidenteve të mundshme të sigurisë.
8.23	Filtrimi i uebit	Ky është një kontroll i ri me kërkesën që përdoruesit të bllokohen nga qasja në faqet e jashtme të internetit që mund të përmbajnë përmbajtje me qëllim të keq ose përmbajtje që nuk është në përpjesëtim me politikat kompaniive.
8.28	Kodimi i sigurt	Kompanitë duhet të sigurojnë që parimet e kodimit të sigurt janë projektuar, zbatuar dhe janë duke u ndjekur gjatë gjithë ciklit jetësor të zhvillimit.

Deklarata e zbatueshmërisë

Deklarata juaj e Zbatueshmërisë (SOA) duhet të përmbajë kontrollet dhe justifikimin e nevojshëm për përfshirjen e tyre, nëse kontrollet e nevojshme janë zbatuar apo jo dhe justifikimin për çdo kontroll të përjashtuar.

Kompanitë duhet të kenë hartuar SOA-në e

tyre me kërkesat e ISO 27001:2022. Përdorimi i atributeve, i cili nuk është i detyrueshëm, mund të prezantohet për të kuptuar më mirë kontrollet dhe mënyrën se si ato trajtojnë fushat e rrezikut të identifikuara nga kompania juaj.

Vlerësimet e rrezikut/regjistrim

Vlerësuesi juaj do të dëshirojë të shohë prova që vlerësimet/regjistrat e rrezikut janë përditësuar për të marrë parasysh kontrollet e reja që janë futur nga ISO 27001:2022.

HAPAT E ARDHSHËM

Duke u përgatitur për Tranzicionin ISO 27001

➢ Kompanitë duhet t'i kalojnë ato sistemin e menaxhimit në përputhje me kërkesat e ISO 27001:2022 përpara se të kryhet auditimi i tyre i tranzicionit.

Kjo duhet të përfshijë çdo ndryshim të dokumentacionit, së bashku me dëshminë e çdo kërkese të re ose të ndryshuar të procesit.

➢ Vlen të përmendet se kompanitë duhet të kryejnë një auditim të brendshëm dhe rishikim të menaxhmentit të kërkesave të reja përpara se të kryhet auditimi i tranzicionit të AQSCERT-së.
➢ Kompanitë mund të kenë një vlerësim të mangësive të tranzicionit të kryer nga AQSCERT përpara auditimit të tyre zyrtar të tranzicionit. Kjo mund të kryhet në lidhje me një mbikëqyrje të mëparshme ISO 27001:2013, ose në çdo kohë tjetër të pavarur përpara auditimit të tyre të tranzicionit.

Auditimi juaj i tranzicionit ISO 27001

➢ Të gjitha kompanitë duhet të kenë një tranzicion auditimi për të konfirmuar zbatimin e standardit të ri. Auditimi i tranzicionit mund të kryhet në lidhje me një auditim ekzistues, ose mund të jetë një auditim i pavarur;

➢ Nëse auditimi i tranzicionit kryhet në në lidhje me një mbikëqyrje ekzistuese (dmth. mbikëqyrja e tranzicionit,) ose auditimi i ricertifikimit (dmth. rivlerësimi I tranzicionit), kohë shtesë do t'i shtohet kohëzgjatjes së auditimit për të mbuluar kërkesat e reja të paraqitura nga ISO 27001:2022;
➢ Nëse kryhet një auditim i pavarur për auditimin e tranzicionit, kohëzgjatja do të llogaritet në bazë të një kompanie individuale.

Shënim: Kohëzgjatjet specifike të auditimit të tranzicionit do të varen nga madhësia e kompaniës suaj dhe kompleksiteti i ISMS. AQSCERT do t'ju këshillojë për kohëzgjatjen specifike të auditimit të tranzicionit

Certifikatat e rishikuara ISO 27001:2022

Ashtu si në çdo auditim, mospërputhjet e identifikuara gjatë një auditimi të tranzicionit do të kërkojnë që të dorëzohet dhe miratohet një plan veprimi korrigjues. Një certifikatë e përditësuar ISO 27001:2022 do të lëshohet pas miratimit të veprimeve korrigjuese.

Lëshimi dhe vlefshmëria e certifikatës së përditësuar ISO 27001:2022 do të jetë si më poshtë:

Mbikëqyrja e tranzicionit:

Kompania me certifikata ekzistuese "E vlefshme deri më datë" edhe në rast të moskalimit me sukses të tranzicionit, certifikata do të ruhet deri me 30-10-2025.

Rivlerësimi i tranzicionit

Një certifikatë e re "E vlefshme deri më datë" do të lëshohet për periudhën trevjeçare të rinovuar.

Tranzicion i pavarur

"E vlefshme deri në datë" ekzistuese e kompanisë do të ruhet.

Tiranë me 04-03-2023