TOPCERTIFIER
www.topcertifier.com

SERVICEMETHODOLOGIE ISO 27001:2013

INFORMATIE BEVEILIGINGSBEHEER SYSTEEM (ISMS)

TOPCERTIFIER
www.topcertifier.com

INLEIDING TOT ISO 27001:2013

ISO 27001:2013 stelt een organisatie in staat informatiebeveiligingsrisico's te identificeren. Rekening houden met dreigingen, kwetsbaarheden, de impact en het beschermen van de organisatie zonder de CIA (Confidentiality Integrity Availability) van informatie in gevaar te brengen door adoptie juiste informatie Beveiligingsbeheersysteem De algemene agenda van ISO 27001:2013 is om behandelen de onderstaande aspecten.

- Zorg voor een model voor het opzetten, implementeren, exploiteren, monitoren, beoordelen en onderhouden en het verbeteren van een informatiebeveiligingsbeheersysteem met fysieke en technische controles.

- Zorg ervoor dat het ISMS wordt geïntegreerd in de bedrijfsprocessen van organisaties.

- Creëer een organisatiecultuur die actieve deelname van medewerkers aan het bedrijf stimuleert Informatiebeveiligingsbeheersysteem.

AFTRAP

De kickoff meeting is een essentieel instrument om te communiceren en plannen te maken voor de uitvoering van het project met minimale belemmering en om het project binnen de geplande tijd en kosten te voltooien. Agenda voor de kick-off bijeenkomst is:

- Bespreking van het projectplan: Dit omvat discussie over de aansprakelijkheid en de verantwoordelijkheid van de inzet houders. mijlpalen en resultaten in het project

- Omvang van de dienstverlening en omvang van de certificering

- Wettelijke en regelgevende vereisten

CREATIE VAN EEN KERNTEAM

- Benoeming van CISO
- Benoeming van het Informatiebeveiligingsbeheerscomité
- Benoeming van interne auditors
- BCP-beheerder
- Benoeming van ISO-leider

TOPCERTIFIER
www.topcertifier.com

GAP-ANALYSE

Tijdens deze fase voeren we een gap-analyse uit om te controleren hoeveel van uw huidige praktijken er in zitten aansluiten bij de standaardeisen. praktijken worden getoetst aan deze vier referentiecriteria

- ISO 27001:2013 standaardvereisten
- SOA
- Wettelijke, statutaire en regelgevende vereisten
- Klantvereisten
- Intern beleid en procedures

De resultaten van deze analyse worden gepresenteerd in de vorm van een Gap Analysis Report. Dit rapport werkt als de lijst met actiepunten ter herinnering aan het project.

ISMS-BEWUSTWORDINGSTRAINING

ISMS awareness trainingen worden gegeven aan de medewerkers van uw organisatie. De opleiding sessie is om medewerkers te helpen kennis op te doen, de concepten van ISO 27001:2013 te begrijpen, en processen en praktijken op één lijn brengen met het oog op het bereiken van een veilige en bedreigingsvrije werkomgeving. Wanneer de medewerkers zijn opgeleid, kunnen zij denken en handelen en bijdragen aan het realiseren van de doelstellingen doelen.

RISICO REGISTREREN & SOA

Er moet een risicobeheerprocedure worden gedocumenteerd en gebruikt als referentie voor het beheer van de risicobeheerprocedure risico's geïdentificeerd in overleg met alle proceseigenaren en functionele hoofden. Wij hanteren ISO31000 & ISO 27005 Risicomanagement standaardtechnieken voor het identificeren, analyseren, evalueren, documenteren, prioriteren, behandelen en kwantificeren van de geïdentificeerde risico's. Met deze stap wordt een risicoregister gemaakt. Geschikt risico behandelplannen worden geïdentificeerd op basis van het risicobereidheidsniveau en de CIA-factor van het bedrijf. De uitkomsten van dergelijke acties worden berekend, vastgelegd, geëvalueerd en gedocumenteerd. De Statement of Applicability (SOA) definieert en identificeert de fysieke en technische controles van toepassing op uw organisatie op basis van uw bedrijfsproces en vereisten.

TOPCERTIFIER
www.topcertifier.com

VERMOGENSBEHEER

Wij helpen bij het ontwikkelen van beleid en procedures voor vermogensbeheer door te coördineren met de functionele hoofden en begrip over het proces. Het hoofddoel van activa beheer is:

- Om de bedrijfsmiddelen van de organisatie te identificeren en passende beschermingsverant woordelijkheden te definiëren

- Om ongeoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van opgeslagen informatie te voorkomen op media

- Ervoor zorgen dat informatie een passend beschermingsniveau krijgt, in overeenstemming met de eisen ervan belang voor de organisatie

NETWERK- / COMMUNICATIEBEVEILIGING:

Wij helpen bij het ontwikkelen van beleid en procedures voor netwerkbeveiligingsbeheer door te coördineren met de functionele hoofden en begrip voor het proces.
Het hoofddoel van netwerkbeveiliging is:

- Het waarborgen van de bescherming van informatie in netwerken en de ondersteunende informatieverwerking ervan faciliteiten

- Om de veiligheid te behouden van informatie die wordt overgedragen binnen een organisatie en waarmee elke externe entiteit

INCIDENTBEHEER

Wij helpen bij het ontwikkelen van beleid en procedures voor incidentbeheer door te coördineren met de functionele hoofden en begrip over het proces. Het hoofddoel van incident beheer is:

- Zorgen voor een consistente en effectieve aanpak van het beheer van informatiebeveiliging incidenten, inclusief communicatie over beveiligingsgebeurtenissen en zwakke punten

TOPCERTIFIER
www.topcertifier.com

BEDRIJFSCONTINUÏTEITBEHEER

Wij helpen bij het ontwikkelen van beleid en procedures voor het beheer van bedrijfscontinuïteit door afstemming met de functionele hoofden en begrip voor het proces. Het hoofddoel van het bedrijfscontinuïteitsmanagement is als volgt:

- Om ervoor te zorgen dat de continuïteit van de informatiebeveiliging wordt ingebed in de bedrijfsvoering van de organisatie continuïteitsmanagementsystemen

- Het garanderen van de beschikbaarheid van informatieverwerkingsfaciliteiten

FYSIEKE VEILIGHEID:

Wij helpen bij het ontwikkelen van beleid en procedures voor fysieke beveiliging door te coördineren met de functionele hoofden en begrip over het proces. Het hoofddoel van Fysiek veiligheid is:

- Om ongeoorloofde fysieke toegang, schade en inmenging in de organisatie te voorkomen informatie en informatieverwerkingsfaciliteiten

- Om verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbrekingen van die van de organisatie te voorkomen operaties

PERSONEELSZEKERHEID:

Wij helpen bij het ontwikkelen van HR-beleid en -procedures door te coördineren met de functionele hoofden en begrip voor het proces. Het hoofddoel van HR-beveiliging is:

- Ervoor zorgen dat medewerkers en opdrachtnemers hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor ze in aanmerking komen

- Het beschermen van de belangen van de organisatie als onderdeel van het proces van verandering of beëindiging werkgelegenheid

- Om ervoor te zorgen dat er adequate training is gegeven aan alle werknemers en leveranciers respect voor informatiebeveiliging

TOPCERTIFIER
www.topcertifier.com

DOCUMENTATIE

Onze experts zullen een overzicht geven van het beleid, de processen, de SOP's, de toepasselijke SOA en de documenten die hieraan moeten voldoen gedefinieerd en gedocumenteerd volgens de vereisten van ISO 27001:2013 door dit met iedereen te bespreken Afdelings- en functiehoofden assisteren wij u bij het opmaken van de benodigde documentatie.

VESTIG ISMS-CONTROLES

Zodra het beleid, de processen, de Statement of Applicability (SOA) zijn controles en SOP's hebben gedocumenteerd en de lijst met te verzamelen gegevens is genoteerd en het personeel is opgesteld geïdentificeerd en getraind in dergelijke activiteiten, dan is het nodig om de activiteiten uit te voeren, te monitoren en te beoordelen efficiëntie van dergelijke processen.

INTERNE AUDITOROPLEIDING

ISO 27001:2013 Interne Auditor (IA) Training zal worden gegeven aan het geïdentificeerde personeel. Deze training zal dergelijk personeel toerusten om de behoefte aan IA te analyseren, IA te plannen en in te plannen, en zich voor te bereiden auditchecklists, en het uitvoeren van een evaluatie, en het documenteren en rapporteren van hun observaties aan de top beheer.

INTERNE AUDIT

Onze experts houden toezicht op de uitvoering van de interne audit door uw interne auditteam. Deze interne audit zal nog bestaande hiaten in het systeem identificeren en het niveau ervan aantonen voorbereiding op de certificeringsaudit. Deze audit geeft de organisatie daartoe de kans alle non-conformiteiten identificeren en corrigeren alvorens over te gaan tot de certificeringsaudit. De bovenkantHet management is op de hoogte van de bevindingen van de interne audit.

TOPCERTIFIER
www.topcertifier.com

OORZAAKANALYSE (RCA) EN CORRIGERENDE ACTIES

Alle non-conformiteiten die zijn vastgesteld tijdens de interne audit, audits van klanten of derden, of van Methodologie voor risicobeoordeling en risicobehandeling, risicoregister Incidentenregister, Kwetsbaarheid Assessment & Penetration Test (VAPT) Rapport, Malware-aanvallen, downtime-register, netwerk problemen, toegangscontroles, activaregister, risicobeoordelingsrapporten van derden, CIA-informatie classificatie, interne en externe aanvallen en alle andere bronnen moeten worden vermeld. RCA te zijn uitgevoerd met behulp van technieken zoals Brainstorming en Fish-Bone-methoden. Het optimale correctiemiddel acties worden uitgevoerd. De effectiviteit van dergelijke acties wordt gedocumenteerd en beoordeeld via een Rapport met corrigerende maatregelen (CAR).

MANAGEMENTREVIEWVERGADERING (MRM)

De MRM is een gelegenheid voor alle ISMS-stakeholders om op geplande tijdstippen bijeen te komen om de bespreek en plan acties op de onderstaande agendapunten.

- Effectiviteit van het huidige managementsysteem met betrekking tot ISMS
- Risicobeoordeling en risicobehandelingsplannen en -registraties
- Resultaten over CIA (Confidentiality Integrity & Availability) van de informatie
- Auditbevindingen en non-conformiteiten uit alle bronnen
- Correctief actieplan om openstaande posten op te lossen
- Voortdurende verbeteringen aan het systeem
- Benodigde middelen en trainingen
- Wettelijke en compliance-aspecten

CERTIFICATIE-AUDIT: FASE 1

Wanneer het paraatheidsniveau een adequaat niveau heeft bereikt, begint het proces voor certificering begint. Een aangewezen auditor van de Certificatie-Instelling (CI) verifieert de Standaard vereisten via een fase 1-audit. Dit houdt in dat de auditor het beleid, de processen, SOP's, SOA, kritische operationele records, IA- en MRM-records. Eventuele grote afwijkingen van de CB's Op dit punt zullen de verwachtingen worden bekendgemaakt, zodat de nodige correcties kunnen worden doorgevoerd. Dit vermindert de kans op grote non-conformiteiten tijdens de certificatieaudit. TOP Certificator zal een contactpersoon zijn met alle belanghebbenden en ziet toe op een vlotte afronding van de audit.

TOPCERTIFIER
www.topcertifier.com

CERTIFICATIE-AUDIT: FASE 2

Na succesvolle afronding van de Fase 1-audit richt de auditor zich op een gedetailleerde audit van het rapport en documentatie van het Information Security Management System van de organisatie. TOPCertifier zou uw personeel met vertrouwen hebben getraind in de auditvereisten geconfronteerd met de audit. Onze experts zullen aanwezig zijn om te helpen met alle middelen die nodig zijn voor een soepel verloop functioneren van de audit. TOPCertifier helpt uw team eventuele non-conformiteiten op te lossen die tijdens de audit zijn vastgesteld. Na succesvolle afronding van de certificatieaudit zal TOPCertifier zal contact onderhouden met alle belanghebbenden om het definitieve certificaat op te stellen, goed te keuren en vrij te geven.

VOORTZETTING VAN NALEVING

TOPCertifier zal deel uitmaken van het compliance-traject van uw organisatie en u regelmatig assisteren intervallen met noodzakelijke trainingen, systeemondersteuning en updates, interne en externe audits en regelmatige verlenging van uw certificering.