ISO 27001 - om att arbeta med systemet.

Bolagsanalys:

Vilka bolag avser att certifiera sig?

Vilket omfång ska den planerade certifieringen ha, så som bolag, avdelningar osv.

Vilken geografiska utbredning har bolaget?

Hur många anställda finns det?

Finns det ett fungerande ledningssystem i dag?

Några mål med ISO certifiering

Etablera ledningssystem

Skapa förstående för organisationen

Sätta ett tydligt scoop

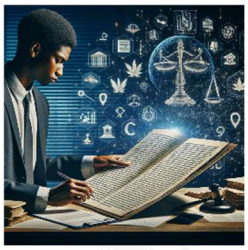
Etablera riskhantiner

Statement of Applicability (SOA)

Kontunituetshantering

Ledningssystem - i stora drag

1. Identifiera, beskriva och uppdatera aktuella **krav och regelverk**.



   Kartläggning av Lagar och Standarder: Börja med att identifiera alla relevanta lagar, förordningar och industristandarder som påverkar din organisation, såsom GDPR, PCI DSS, eller HIPAA.

   Uppdateringsmekanism: Implementera en process för att kontinuerligt övervaka och uppdatera dessa krav, t.ex. genom prenumerationer på juridiska uppdateringar eller genom att använda specialiserade rättsliga tjänster.

   Dokumentation: Skapa och underhåll dokumentation som tydligt beskriver hur dessa krav och regler tillämpas inom organisationen.

2. Identifiera och kategorisera bolagets **informationstillgångar**.

   Tillgångsinventering: Skapa en omfattande lista över alla informationstillgångar, inklusive fysiska enheter, mjukvara, data och intellektuellt kapital.

   Kategorisering: Kategorisera tillgångarna baserat på deras värde, känslighet och kritikalitet för organisationen.

   Ägandeskap: Tilldela ägande för varje tillgång och definiera ansvarsområden.

3. Genomföra **riskanalyser** och besluta om **skyddsmekanismer**.

   Riskbedömningsmetodik: Använd en standardiserad metodik för att identifiera och bedöma risker, som ISO 31000 eller NIST:s ramverk.

   Prioritering: Prioritera risker baserat på deras potentiella påverkan och sannolikhet.

   Beslut om Åtgärder: Välj lämpliga skyddsåtgärder för att minska identifierade risker till en acceptabel nivå, och dokumentera beslutsprocessen.

4. Upprätta organisatoriska **roller** och **ansvarsområden**.

   Rolldefinitioner: Definiera tydliga roller och ansvarsområden för informationssäkerhet, inklusive en Informationssäkerhetschef (CISO) eller liknande position.
   Utbildning och Medvetenhet: Se till att all personal är medveten om sina roller och ansvar gällande informationssäkerhet.
   Kommunikationsplan: Upprätta effektiva kommunikationskanaler för säkerhetsrelaterade frågor.

5. Identifiera och **säkra interna** och **externa processer**, samt **leverantörer** med inriktning mot informationssäkerhet.

   Processkartläggning: Identifiera alla processer som påverkar informationssäkerheten, både interna och externa.
   Leverantörsbedömningar: Genomför regelbundna säkerhetsbedömningar av leverantörer och tredjepartspartners.
   Processförbättringar: Implementera och övervaka kontroller för att säkerställa att processerna uppfyller säkerhetskraven.

6. Upprätta och underhåll dokumentation för att **säkerställa adekvat styrning**.

   Policyer och Procedurer: Utveckla och dokumentera policyer och procedurer för informationssäkerhet.
   Dokumenthantering: Se till att all dokumentation är aktuell, tillgänglig och skyddad.
   Revisionsmekanismer: Implementera processer för regelbundna interna och externa revisioner av ISMS-dokumentation och praxis.

ISO 27000 relaterat

Dataintrång och Cyberattacker : Revisionsbolag hanterar ofta konfidentiell och känslig information, vilket gör dem till attraktiva mål för cyberattacker. Detta inkluderar risker som ransomware, phishing, och andra former av skadlig programvara.

Dataskydd och Sekretess : Fel i hanteringen av personuppgifter kan leda till brott mot dataskyddslagar som GDPR. Det är viktigt att skydda klientinformation och andra personuppgifter mot otillåten åtkomst och läckage.

Intern Säkerhet: Internt orsakade säkerhetsincidenter, vare sig av misstag eller genom illasinnade handlingar, är en betydande risk. Detta inkluderar felaktig hantering av data, otillräcklig tillgångskontroll och interna datastölder.

Teknisk Sårbarhet och Systemfel : Otillräckliga säkerhetsuppdateringar, svagheter i IT-systemen eller fel i mjukvara och hårdvara kan leda till betydande säkerhetsproblem.

Compliance och Regelverksföljsamhet : Att inte följa lagar och standarder som ISO 27001 kan leda till rättsliga påföljder, böter och förlorad kundtillit.

Kontinuitetsplanering och Katastrofåterställning: Brister i planering för hur verksamheten ska fortsätta vid en större incident (t.ex. naturkatastrofer, brand, eller större tekniska fel) kan ha allvarliga konsekvenser för företagets förmåga att fortsätta sin verksamhet.

Tredjepartsrisker: Risker associerade med underleverantörer och andra externa parter som revisionsbolaget är beroende av. Detta inkluderar risker relaterade till deras säkerhetspraxis och datahantering.

Policys bör spänna över dessa områden:

Affärsverksamhet och Lokaliseringsområden: Identifiera vilka delar av organisationen eller vilka processer som ska inkluderas i ISMS. Det kan vara hela organisationen eller specifika avdelningar, platser eller tjänster.

Informationstillgångar: Bestäm vilka informationstillgångar som ska skyddas. Detta kan inkludera allt från fysiska dokument till digital data, programvara och hårdvara.

Riskbedömning och Riskhantering: Genomför en riskbedömning för att identifiera och bedöma risker för organisationens informationstillgångar. Riskhanteringsstrategier bör sedan utvecklas för att hantera identifierade risker.

Rättsliga, Regulatoriska och Kontraktsmässiga Krav: Identifiera och säkerställ efterlevnad av alla relevanta lagar, förordningar och kontrakt som påverkar organisationens informationssäkerhet.

Säkerhetspolicy och Mål: Utveckla en säkerhetspolicy som stöder organisationens övergripande affärsmål och säkerställer att säkerhetsmålen är i linje med denna policy.

Mänskliga Resurser: Ta hänsyn till roller och ansvar för personalen inom ISMS, inklusive utbildning, medvetenhet och kompetensutveckling.

Processer och Procedurer: Etablera och underhålla processer och procedurer för att stödja och upprätthålla ISMS.

Kontinuerlig Förbättring: ISO 27001 kräver ett åtagande om kontinuerlig förbättring av ISMS. Detta innebär regelbundna översyner och uppdateringar av systemet för att säkerställa dess effektivitet.

Intern och Extern Kommunikation: Bestäm hur information om ISMS ska kommuniceras internt inom organisationen och externt till intressenter.

Nödläge och Återhämtning: Inkludera planer för att hantera säkerhetsincidenter och återhämtning efter händelser.

Det är viktigt att komma ihåg att ISO 27001-certifiering inte bara är en engångshändelse utan kräver kontinuerligt engagemang och underhåll för att säkerställa att ISMS förblir effektiv och uppdaterad med föränderliga risker och förhållanden.