Ledningsystem

Presentation

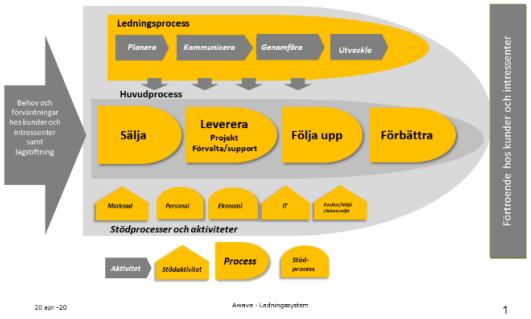
Awave AB med tillhörande företag är certifierade av SCAB enligt SS-EN ISO 9001:2015 och 14001:2015 och slutför nu i april/maj införandet av SS ISO/IEC 27001:2014 Ledningssystem för informationssäkerhet samt SS-EN ISO 22301:2014 Ledningssystem för kontinuitet.

Standardkraven är integrerade i verksamheten och dokumenterade i manualer för ledning, leverans, säkerhet, kontinuitet och arbetsmiljö. Effekterna av ledningssystemet redovisas löpande vid projektledningsmöten samt i en avvikelselogg för hela verksamheten och periodiskt i en SWOT och intressentanalys, protokoll för ledningens genomgång, kundnöjdhetsutvärderingar, risk- och sårbarhetsbedömningar av aktiviteter och av tillgångar för att sätta risknivåer, interna revisioner och i den ekonomiska redovisningen.

Verksamhetens ledningssystem utgår från en övergripande processkarta nedbruten i processer, aktiviteter och rutiner. Varje process följer processcykeln ”Plan-Do-Check-Act”.

Varje integrerad aspekt, kvalitet, informationssäkerhet, kontinuitet, miljö och arbetsmiljö har sin egen policy baserad på verksamhetsidén. Ansvar för att dessa följs och utvecklas samt riskvärderas har respektive processägare tillika ägare av informationstillgångarna.

Verksamhetens processer och aktiviteter



Ledningsprocessen omfattar verksamhetsplanering vari ingår planering av marknadsaktiviteter, kundfokus, riskanalyser av/i verksamheten, informationssäkerhet inklusive kontinuitet (SoA), miljö och arbetsmiljö samt kompetensutveckling.

Huvudprocessen innehåller försäljning, leverans och uppföljning/förbättring. Kundbehoven kartläggs med kunden. Ett projekt startas upp, planeras, riskbedöms, designas, utvecklas, testas och går ”live” efter kundgodkännande. Efter leverans utvärderas prestandan och om kunden vill så tecknas ett ”förvaltningsavtal” som även det följer en inarbetad projektstruktur och med kunden överenskomna aktiviteter.

Stödprocesserna omfattar marknadsföring, ekonomi, personal (HR), IT och systemansvar. Genom HR säkerställs personsäkerheten och genom IT samt Ledning att IT-systemet är tekniskt och organisatoriskt säkert. En funktion för systemansvar (kvalitet, miljö och arbetsmiljö) genomför planerade interna revisioner utifrån samtliga standarder som rapporteras vid mötet för ”Ledningens genomgång”.

Informationssäkerhet - policy

Awave är en IT-och webbyrå med bred teknisk kompetens, som erbjuder en stor kundkrets av varierande storlek och branscher, digitala lösningar inom webb, e-handel och appar med tillhörande kringtjänster.

Tjänsterna levereras av en certifierad kvalitets- och miljöledd verksamhet med en datamedveten och kunnig personal i en säker och kontinuitetsplanerad drift i skyddade lokaler. Av detta följer att vi

- väljer lämplig kommunikation och säkerhet beroende på uppdrag, kund och intressent,
- styr och övervakar datan i egna och intressenters system,
- riskbedömer processer och de verktyg som krävs,
- uppfyller krav på informationssäkerhet, som granskas revideras och förbättras planenligt,
- hanterar och skyddar informationstillgångarna,
- säkerställer personsäkerheten i samband med säkerhetskrav i arbetsuppgifterna,
- utbildar och tilldelar personalen definierade ansvar och befogenheter i informationssäkerhet.

Med hjälp av vårt ledningssystem för informationssäkerhet åtar sig Ledning och övriga medarbetare att uppfylla kunders och intressenters krav på informationssäkerhet, att uppfylla mål, författningskrav och avtalsvillkor samt att arbeta med ständiga förbättringar.

Stockholm 26 februari 2020

Carl-Johan Beckman

CEO

Ledningsystem

Presentation

Ledningssystem för information (LIS)

Genom ledningssystemet finns processer och rutiner att följa som underlättar riskanalyser.

För att säkerställa att alla standardkriterierna beaktas följer vi Annex A, State of Applicability i ISO 27001.

Alla informationstillgångar (organisation, processer, personal, kompetenser, tjänster som köps in och som erbjuds, produktionsutrustning och fysiska faciliteter) har identifierats och värderats samt riskklassificerats. För tillgångar med medel och hög risknivå har införts inplanerade uppföljningar och kontroller.

LIS följer samma processmodell som för övriga tillämpade standarder.

Följande principer för skydd och åtgärder tillämpas.

- Informationstillgångarna identifieras och kategoriseras,
- Riskbedömning görs av samtliga informationstillgångar,
- För informationstillgångar med riskvärde över en viss nivå vidtas åtgärder och upprättas rutiner för skydd (steg 1),
- För prioriterade informationstillgångar förfinas riskanalysen (steg 2),
- Riskbedömningarna och upprättad kontrollinformation dokumenteras, implementeras och övervakas,
- Avvikelser loggas, sammanställs och rapporteras vid ”ledningens genomgång”.
- Dokumenterad information (”manualerna”) uppdateras vid behov och efter interna och externa revisioner.

Ledningssystem för kontinuitet (”BCM”)

I ledningssystemet finns processer och rutiner att följa som underlättar riskanalyser. Kontinuitet är en parameter vid värdering och riskbedömning av informationstillgångarna. BCM följer LIS som kompletterats med rutiner för kontinuitetssäkring och en BCP dvs. en Avbrotts- och kontinuitetsplan innehållande:

- Krisorganisation
- Avbrott
- Konsekvenser och förebyggande åtgärder
- Reservrutiner
- Återgång till normal drift
- Förvaltning och underhåll av BCP
- Kontinuitetsrutiner
- Dokumentstyrning

Följande principer för skydd och åtgärder tillämpas.

- Informationstillgångarna identifieras och kategoriseras,
- Riskbedömning och bedömning av acceptansnivå för avbrott görs av samtliga informationstillgångar,
- För informationstillgångar med riskvärde över en viss nivå (kritikalitet för leverans och kontinuitet) vidtas åtgärder och upprättas rutiner för skydd (steg 1)
- För prioriterade informationstillgångar (kritikalitet för leverans och kontinuitet) förfinas riskanalysen (steg 2)
- Riskbedömningarna och upprättad kontrolldokumentation dokumenteras, implementeras och övervakas,
- Avvikelser loggas, sammanställs och rapporteras vid ”ledningens genomgång”.
- Avbrotts- och kontinuitetsplanen uppdateras vid behov och efter interna revisioner.