

MiniGuide

Roller och processer för IT & Informationssäkerhet

IT- & Informationssäkerhet



IT Ledarskap

Vi erbjuder spjutspetskompetens med hög integritet för att hjälpa företag och organisationer till ett effektivt utnyttjande av IT med målsättning att verksamhetsprocesser skall leverera och skapa värde.

Introduktion

För alla verksamheter är information en viktig tillgång och förutsättning för att driva verksamheten. När vi i detta sammanhang talar om IT- och Informationssäkerhet avser det att skydda Sekretess, Riktighet och Tillgänglighet till information och informationstillgångar.

För att hantera detta bör man utgå ifrån riskanalyser som är ett stöd vid prioritering av vad som måste skyddas i första hand och i vilken ordning man skall vidta säkerhetsåtgärder.

Roll som äger frågan

Hur man hanterar ansvaret för IT- och Informationssäkerhet varierar beroende på organisationens storlek och bransch. Den första frågan man måste ta ställning till är om man vill att rollen skall finnas i eller utanför IT organisationen.

Vill man ha kontroll över IT är det vanligt att denna roll finns inom Risk Management, kvalitetsorganisationen eller annan stödjande del i verksamheten. Här man istället som målsättning att säkerhetsarbetet skall vara en integrerad del i den operativa verksamheten är det inte ovanligt att det är en del inom IT organisationen. I det sistnämnda fallet blir det dock väldigt svårt att anmärka på säkerhetsbrister.

Processer

Arbetet med IT- och Informationssäkerhet innebär i grunden att etablera regler och se till att dessa efterlevs. Går man lite mer på djupet kan man identifiera några grundläggande processer som bör beaktas:

- Analysera risker
- Etablera säkerhetskrav och åtgärder
- Säkerhetsgodkänna ändringar
- Hantera incidenter
- Säkerställ kontinuitet
- Skapa medvetenhet
- Verifiera efterlevnad

Det är även vanligt att några av dessa processer delas upp ytterligare:

- Hantera behörigheter
- Hantera extern åtkomst

ISO/IEC 27000 serien

Den nuvarande ISO 27K (tjugosjutusen) serien har sitt ursprung i den brittiska standarden BS7799. Som ISO standard fick den benämningen ISO/IEC 17799 initialt och 2005 publicerades den första delen som: "ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements"