

**Vad betyder policy**  
Ett begrepp som används på flera håll i ISO/IEC 27001 är ordet "policy". Innebörden av ordet är en argumentation eller en aktivitetsplan som gäller för en individ eller en grupp.

Inom vart och ett av dessa områden finns det mer detaljerade undergrupperingar.  
Inom vart och ett av dessa områden finns det mer verksamheten samt Efterlevnad.  
tionssäkerhetsincidenter, kontinuitetsplanering för håll av informationssystem, Hantering av information av åtkomst, Anskaffning, utveckling och under- säkerhet, Styrning av kommunikation och drift, Styr- sonalresurser och säkerhet, Fysisk och miljörelaterad informationssäkerheten, Hantering av tillgångar, Per- tioner omfattar: Säkerhetspolicy, Organisation av De områden som är relevanta för de flesta organisa- tioner omfattar: Säkerhetspolicy, Organisation av informationssäkerheten, Hantering av tillgångar, Per- sonalresurser och säkerhet, Fysisk och miljörelaterad säkerhet, Styrning av kommunikation och drift, Styr- ning av åtkomst, Anskaffning, utveckling och under- håll av informationssystem, Hantering av informa- tionssäkerhetsincidenter, kontinuitetsplanering för verksamheten samt Efterlevnad.  
En effektiv tillämpning av ISO/IEC 27001 utgår ifrån riskbedömning, analys av lagar och regler som påverkar verksamheten samt analys av de verksamhetskrav som finns. Med stöd av detta är det möjligt definiera åtgärdsåtgärder och säkerhetsåtgärder som tillför värde.  
De områden som är relevanta för de flesta organisa- tioner omfattar: Säkerhetspolicy, Organisation av informationssäkerheten, Hantering av tillgångar, Per- sonalresurser och säkerhet, Fysisk och miljörelaterad säkerhet, Styrning av kommunikation och drift, Styr- ning av åtkomst, Anskaffning, utveckling och under- håll av informationssystem, Hantering av informa- tionssäkerhetsincidenter, kontinuitetsplanering för verksamheten samt Efterlevnad.

#### 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.

**Plan** (Upprätta) Handlar om att göra avgränsningar, ta fram policy, etablera riskbedömning och välja åtgärdsåtgärder.  
**DO** (Införa och driva) Innebär att arbeta med stöd av en riskhanteringsplan, för att införa säkerhetsåtgärder och sprida budskapet.  
**Check** (Övervaka och granska) Övervaka och kontrollera att regler är effektiva och att de efterlevs.  
**Äkt** (Underhålla och förbättra) Omfattar att systematiskt samla upp förbättringsförslag, vilka bedöms och prioriteras för att kunna införas på bästa möjliga sätt.

#### Att upprätta ett ledningssystem enligt 27001

**Introduktion**  
När man börjar att prata om IT säkerhet, framträder oftast ISO/IEC 27001 standarden som den naturliga referenspunkten. Det finns idag väldigt många företag och organisationer som använder standarden som utgångspunkt för det egna säkerhetsarbete, men endast ett fåtal har valt att uppnå certifiering.  
Har verksamheten erfarenhet av ISO 9000 kan ISO/IEC 27001 användas som ett komplement. Det skapar också möjlighet att koppla säkerhetsåtgärder till verksamhetsprocesser.  
Med utgångspunkt från Plan-Do-Check-Act metodiken innebär ett införande följande:

## MiniGuide

IT- och informationssäkerhet  
med stöd av ISO/IEC 27001

IT- & Informationssäkerhet

