

## ISO/IEC 27000 IT- och Informationssäkerhet

### Riskmedvetenhet är nyckeln

Säkerhet handlar om att **bevara sekretess, integritet och tillgänglighet avseende information**. Säkerhet i sin tur innebär att hantera risker där det är nödvändigt att arbeta med riskanalyser, där dessa identifieras och bedöms.

### Etablera IT- och informationssäkerhet

Framgångsfaktorn är medvetenhet och förankring hos alla medarbetare och att säkerhetsarbetet är en naturlig del i arbetet.

Det är ofta komplext och kan upplevas som att säkerhet endast berör "säkerhetsfolket". För att få spridning i organisationen ger Enterprise Pilot det stöd du behöver.

### Snabbt komma igång

Vi **rekommenderar** som första steg en **översiktlig analys** av nuvarande säkerhetsåtgärder mot de föreslagna i ISO/IEC 27001 samt en analys av era verksamhetsprocesser och er organisationsstruktur.

### Kontinuerliga förbättringar

Oavsett om man väljer att certifiera sig enligt ISO/IEC 27001:2006 eller ej, följer ett arbete med kontinuerliga förbättringar. Detta arbete utgår ifrån rapporteringen av avvikelser, incidenter och brister samt uppdatering av befintliga riskanalyser, för att spegla aktuella förutsättningar.

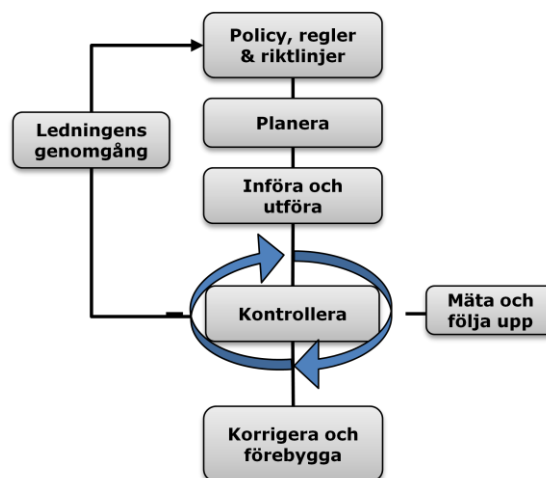
Vid införande av ISO 27000 med stöd av Enterprise Pilot, baseras vårt angreppssätt ifrån Deming's Plan-Do-Check-Act process. De aktiviteter som är aktuella anpassas till rådande förutsättningar.

**Vinsten** är att fortsatt vara den tillförlitliga part som era kunder känner tillit till. Genom att minimera oförutsedda händelser, minska kostnaderna och behålla goda relationer baserat på verklig förmåga.

### Fördelarna är;

- Samlar säkerhetspolicy och säkerhetsåtgärder på en plats
- Kopplar kraven med verksamhetens processer
- Enkel att använda – lätt att uppdatera
- Ger rätt personer rätt och relevant information om säkerhetskrav
- Underlättar vid revisioner

**Nulägesanalysen ligger sedan till grund för att ta fram en väl anpassad och effektiv införande plan.** Vi har även erfarenhet av att hjälpa företag att certifiera sig enligt ISO/IEC 27001:2006.



## Deming's Plan-Do-Check-Act process

Huvuddragen är:

**Plan:** Analysera verksamhetsprocesser och identifiera intressenter, ta fram säkerhetspolicy, ta fram riskanalysmetod, gör riskanalys och ta ställning till hur risker skall hanteras. Vill ni även certifiera er enligt ISO/IEC 27001 tas även ett uttalande om tillämplighet fram.

**Do:** Utveckla säkerhetsåtgärder respektive systemlösningar som skall stödja dessa åtgärder. Införande i verksamheten.

**Check:** Löpande avvikelserapportering samt internrevisioner och granskningar för att verifiera efterlevnad.

**Act:** Genomför åtgärder som föreslås i avvikelserapportering och revisionsrapporter samt genomför förbättringsförslag från medarbetarna som är drivare till förändring

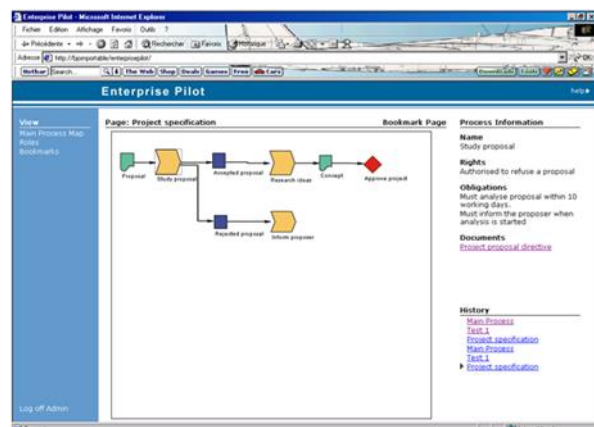
## Enterprise Pilot

Med Enterprise Pilot får du ett **lättanvänt ledningssystem**. Du kan skapa ert eget unika säkerhetsarbete utifrån ISO 27000 och integrera säkerhetsåtgärderna i era befintliga verksamhetsprocesser.

Är ni redan ISO 9000 certifierade kan du koppla samman säkerhetsåtgärderna för att få ett gemensamt och heltäckande ramverk för både ISO 9000 och ISO 27000.

Enterprise Pilot är en webbaserad tjänst för att dokumentera och publicera processbaserade ledningssystem med tillhörande instruktioner och mallar, som följer kvalitetsstandarderna dvs. med automatisk versionshantering och spårbarhet.

Mer finns att läsa på [www.enterprise-pilot.se](http://www.enterprise-pilot.se)



## Kontakt information

Gefwert Development;  
Marie-Louise Gefwert  
[marie-louise@gefwert.se](mailto:marie-louise@gefwert.se)  
070-644 90 80  
[www.gefwert.se](http://www.gefwert.se)

Scillani Information AB;  
John Wallhoff  
[john.wallhoff@scillani.se](mailto:john.wallhoff@scillani.se)  
070- 774 31 31  
[www.scillani.se](http://www.scillani.se)