



## MÄTNING AV INFORMATIONSSÄKERHET

## Ska ni införa eller förbättra LIS?

### STÖD VID INFÖRANDE ELLER FÖRBÄTTRINGAR AV LIS

Strävar ni efter att följa ISO/IEC 27001, den internationella standarden för informationssäkerhetsledning? Tänker ni införa ett ledningssystem för informationssäkerhet (LIS), eller har ni ett existerande LIS som behöver förbättras?

Då är Veriscan Basic det rätta verktyget för er!

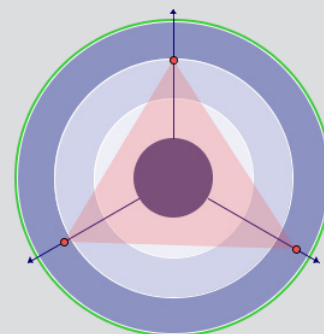
Veriscan Basic omfattar en metod och ett verktyg för att genomföra en gapanalys, för att ta vara på existerande processer och rutiner i verksamheten, så att man lätt kan se vad som behöver kompletteras för att följa standarden.

### MÄTPROGRAM BASIC

Veriscan Basic™ är en gapanalys som ger en detaljerad handlingsplan för att organisationer ska kunna bli certifierbara mot ISO/IEC 27001.

Veriscan Basic kan användas som en enskild tjänst, men den kan också med fördel kombineras med ett LIS-införande med hjälp av Veriscan Security. Som projektstöd rekommenderas Veriscans egenutvecklade programvara, Vake.

Det finns möjlighet till en förkortad variant på Veriscan Basic, där förbättringsförslagen utesluts och då blir att betrakta som en nulägesanalys.



### Veriscan Basic visar vägen framåt

Veriscan Basic bygger på Veriscan Rating som är en patenterad metod för mätning av informationssäkerhet.

Mätningen ger en tydlig bild över säkerhetsnivåer inom de tre områden som informationssäkerhet omfattar:

- Organisatorisk säkerhet
- Fysisk säkerhet
- Systemsäkerhet (ICT-säkerhet)

Veriscan Basic har en tydlig koppling till ISO/IEC 27001, där kategoribenämningar stämmer överens med Bilaga A:s kapitelindelning. På detaljnivå finns i Veriscan Basic minst en mätpunkt för varje säkerhetsåtgärd i standarden. För att fånga hela omfånget i standarden har en egen kategori skapats, som innehåller mätpunkter mot de krav i standarden som inte omfattas av Bilaga A.

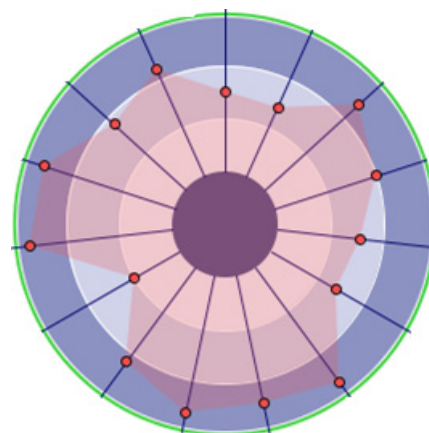
Genom indelning i områden, kategorier och mätpunkter har er organisation möjlighet att få en djup förståelse över nuläget för informationssäkerhet oavsett vilken nivå i organisationen man befinner sig på.

## VERISCAN BASIC OCH RATING METODIKEN

Veriscan Basic genomförs som en välplanerad intervju-session med utvalda roller i en organisation, som därmed utan större ansträngning får handfasta förslag på de åtgärder som ska föra organisationen närmare en certifiering eller närmare de mål som organisationen har satt upp för sin informations-säkerhet.

Veriscan Basic hör till Veriscan Rating® familjen, på så vis att samma verktyg och utvalda delar av samma metodik används. Men medan Veriscan Rating passar för en organisation som redan har ett väletablerat LIS, så lämpar sig Veriscan Basic för en organisation som tänker införa ett LIS, eller som har ett LIS som inte fungerar som det är tänkt.

### BASIC RESULTAT GRAFISK BILD



## RESULTATET AV EN VERISCAN BASIC

Veriscan Basic ger både en övergripande bild av en organisations status gentemot ISO/IEC 27001 och en detaljerad beskrivning motsvarande varje säkerhetsåtgärd i standarden (Bilaga A).

Två nivåer av rapporter levereras. Analysrapport med sammanfattningar för varje område och kategori som framförallt vänder sig till ledningen. Mät-punktsrapport, där detaljerna framgår som vänder sig till roller ansvariga för informationssäkerhet samt till de roller som blir direkt ansvariga för att genomföra åtgärder, inklusive projektledning.

Resultaten presenteras även grafiskt, på ett sätt som lämpar sig för en snabb överblick och en snabb insikt om arbetet som återstår för att nå målen.

## EFTER BASIC-MÄTNINGEN

Medan Veriscan Basic ofta är en engångsmätning i en organisation, finns Veriscan Rating för kontinuerlig mätning av informationssäkerheten för att uppnå en god informationssäkerhetsnivå, eller för att gradvis förbättra säkerheten inom specifika områden.

Indelningen i kategorier möjliggör en grafisk sammanställning över statusen för respektive kapitel i ISO/IEC 27001, Bilaga A, samt de kapitel i standarden som innehåller krav som inte omfattas av Bilaga A.

Mätprogrammet är uppdaterat för att stämma överens med 2013 års utgåva av ISO/IEC 27001.