# *Vilket IT-säkerhets ramverk borde mitt företag använda?*

***Av Gustaf Edeby***

***26-09-2023***

## Introduktion

Med tiden har flera datasäkerhetsramverk uppkommit för att hjälpa företag skydda sig mot extern och interna hot. Men vilket ramverk passar just din verklighet och dina uppgifter bäst? Hur ser det ut på marknaden, och hur väljer man så att det skapar bäst värde och möjliggör framtida val och utvecklingar? I detta blogginlägg går vi igenom ett flertal populära ramverk och vad man ska tänka på när man väljer ett ramverk.

## *Populära ramverk*

Bilden nedanför har kända ramverk utplacerade utifrån bredd och applicerbarhet. Den beskriver varje ramverks täckning och applicerbarhet, vilket betyder hur många områden dom täcker med sina rutiner och vilka situationer dom kan appliceras till. Exempelvis är amerikanska HIPAA lagen fokuserad på känslig patientinformation, så arbetar du inte inom den branschen kan den inte användas, medan Essential 8 från australiensiska myndigheter är väldigt bred och kan appliceras i princip alla situationer, men fokuserar mer på fundamentala koncept och inte detaljer.

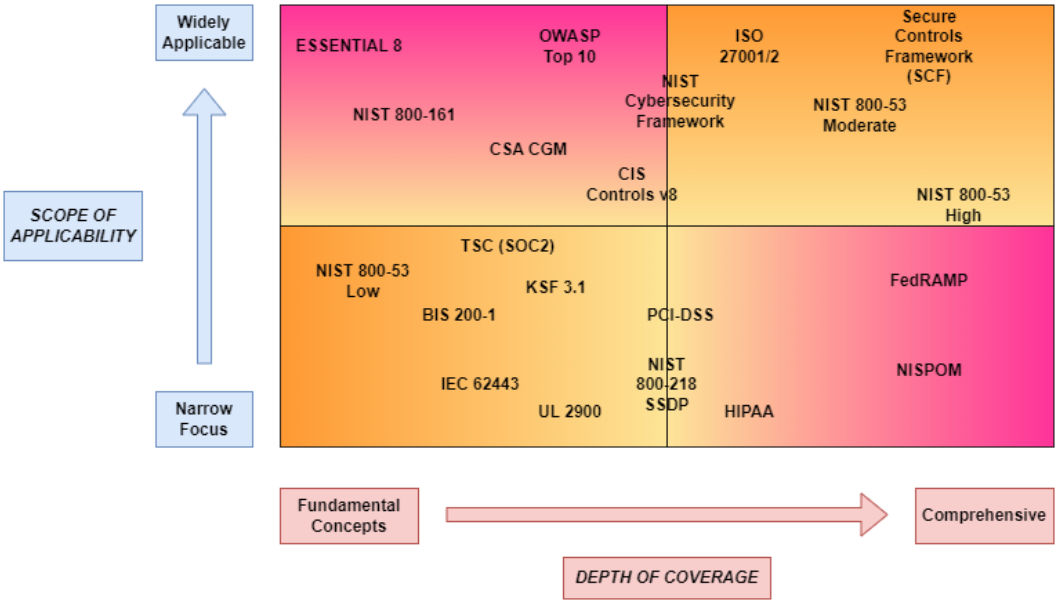


*Bild 1: Jämförelse mellan olika datasäkerhetsramverk.*

Dom bredare ramverk har rutiner för allt inom en organisation, som till exempel ledning, skydd av information och säkerhetsrutiner för anställda. Fokuset i detta inlägg är på dessa bredare ramverken beskrivna nedanför, men det finns andra ramverk som kan vara relevanta för just din organisation.

- ISO27002
- NIST Cybersecurity Framework
- CIS Controls
- KSF 3.1

**ISO27002**

Detta ramverk är en del av 27000-serien. ISO/IEC 27001 är definitionen av ett ledningsinformationssäkerhetssystem (LIS), kallat ISMS på engelska, som man kan certifiera sig mot. ISO/IEC 27002 är ett brett ramverk med stor applicerbarhet som innehåller råd och riktlinjer för att eventuellt certifiera sig mot 27001. Att vara ISO-compliant eller certifierad är ett sätt att påvisa för kunder att din organisation har fullgod datasäkerhet.

Den senaste versionen (ISP 27002:2022) innehåller fyra kategorier med 93 kontroller totalt.

*Organisational controls (Organisationskontroller)*, hanterar ledningssidan av datasäkerhet, skydd av information och kontroller som ej täcks av resterande kategorier.

*People controls (Människokontroller)*, refererar till de mänskliga aspekterna, till exempel säkerhetsträning och distansarbete.

*Physical controls (Fysiska kontroller)*, hur man skyddar fysiska tillgångar, som servrar eller fysisk information.

*Technological controls (Tekniska kontroller)*, IT-sidan av din organisation.

Att implementera ISO 27002 kan gå relativt fort, beroende på hur mogen din organisation är för en implementation. Har ni implementerat LIS för andra ISO-standarder, kan man nyttja dessa rutiner och arbetssätt för att skynda på processen. Bland annat krävs det utvecklandet av policys och rutiner, en sårbarhetsevaluering (risk assessment) och träning av personal för en ISO27002 implementering.

**NIST Cybersecurity Framework**

Designad av amerikanska NIST för kritisk infrastruktur, men har öppnats för publik användning. Ramverkets kontroller är indelade i fem olika ”functions” (funktioner):

*Identify (Identifiera)*, utveckla ledningsfunktionalitet för att hantera risker mot system, människor, tillgångar och data.

*Protect (Skydda)*, utveckla skydd för kritiska tillgångar.

*Detect (Detektera)*, utveckla och implementera skyddsåtgärder för att identifiera ett intrång.

*Respond (Reagera)*, utveckla resurser för hantering av intrång.

*Recover (Återhämtning)*, utveckla planer för redundans och för att återställa funktioner som kan ha blivit påverkade av ett intrång.

Ramverket använder "Tiers" (Nivåer) för att hjälpa organisationer förstå vilken nivå man ligger på. Dessa är:

- Partial (Partiell) – Nivå 1
- Risk Informed (Riskinformerad) – Nivå 2
- Repeatable (Repeterbar) – Nivå 3
- Adaptive (Adaptiv) – Nivå 4

NIST rekommenderar alla organisationer på nivå 1 att implementera, som minst, nivå 2.

Enligt NIST kan en implementation ta flera veckor eller flera år beroende på din organisations storlek, resurser och behov. Det viktigaste är att undersöka vilka rutiner man har för tillfället, vilken nivå man vill nå och genomföra en gapanalys för att se vad man saknar eller måste förbättra. När det är avklarat kan man se hur mycket tid och resurser som krävs för att ni sitt uppsatta mål.

**CIS Controls v8**

CIS Controls är en uppsättning kontroller skapade för att verifiera en organisations IT-säkerhet. Kontrollerna är modulerade för enkel applicering, och de individuella kontrollerna är utförligt skrivna för enkel applicering.

Kontrollerna är uppdelade i 3 nivåer, som kallas "IG" (Implementation Group). Din organisations storlek och krav bestämmer din nivå.

- IG 1: 56 kontroller
- IG 2: 130 kontroller
- IG 3: 156 kontroller

Att implementera CIS kontrollerna är enklare än större ramverk, som CSF, KSF och ISO27002. Det är ett bra steg när en organisation behöver gå från ingen till lite IT-säkerhet till att implementera ett större ramverk. Genom att tillsätta en person eller utomstående organisation att gå igenom CIS kontrollerna mot er organisations IT-policy, kan man enkelt se vilka områden kräver förbättringar.

**KSF 3.1**

KSF (Krav SäkerhetsFunktioner) är ett ramverk framtaget av Försvarsmakten, vars syfte är att sätta säkerhetskrav på upphandlade IT-system. KSF innehåller 148 krav fördelat över sju säkerhetsfunktioner (*funktionella säkerhetskrav)* samt 275 krav på hur man påvisar förtroende för säkerhetsförmågorna (*assuranskrav)*.

De sju grundläggande säkerhetsfunktionerna är:

- Behörighetskontroll (Behörighetskontroll)
- Säkerhetsloggning (Spårbarhet)
- Skydd mot skadlig kod (Antivirus)
- Intrångsdetektering (IDS)
- Intrångsskydd (IPS)
- Skydd mot röjande signaler (RÖS-skydd)
- Skydd mot obehörig avlyssning (Konfidentialitet och sekretess)

Det kan även tillkomma krav vars ursprung är från analyser utanför KSF. Till exempel

- Verksamhetens krav på tillgänglighet
- Författningskrav som gäller för verksamheten som ska använda systemet
- Hotrelaterade krav som är unika för den miljön systemet ska användas i

Att implementera KSF till ett IT-system är ett stort åtagande, då det inte enbart handlar om att utveckla ett säkert IT-system. Utan också att *bevisa* att IT-systemet är säkert (assurans). Det kräver komplexa tester som kan bevisa att säkerhetsfunktionaliteten fungerar korrekt. Om man inte specifikt arbetar mot Försvarsmakten eller andra organisationer som kräver KSF-implementerat så skulle vi ej rekommendera att implementera detta ramverk.

## Hur vet jag vilket ramverk som är rätt för mig?

Alla organisationer har olika kravbild som beror på kunder, partners, teknik, personal och tillgänliga resurser. Att välja vad, och hur, kan vara utmanande frågor. Det du kan göra är att ställa dig följande:

*Måste vi efterleva ett ramverk (vara compliant)?*

Ett mindre företag behöver möjligtvis inte vara compliant till ett specifikt ramverk. En ISO27 001 certifiering kan kosta flera hundra tusen kronor, och är giltigt i 3 år, efter det krävs en om-certifiering. Även om man använder ett ramverk man inte kan officiellt certifiera sig mot, så måste avsevärd arbetstid läggas ned. Investeringen måste därför avvägas mot förtjänsten av att vara compliant.

*Har vi krav på oss att vara compliant till ett specifikt ramverk?*

Större företag har på senare år krävt att leverantörer också ska vara certifierade, eller på annat sätt uppvisa att dom uppfyller strikta säkerhetskrav. Om du är en leverantör, så kan din kund ha krav på att till exempel vara ISO27001 certifierad. Om ert företag arbetar i en leverantörsroll, eller vill expandera in i en annan marknad kan det vara bra att undersöka om de större företagen har krav på leverantörer med. Att vara compliant i det fallet kan ge tillgång till mer kunder, och därmed större vinst.

*Vilket ramverk passar våra mål och behov bäst?*

Om dina kunder är mestadels amerikanska företag kan NIST CF ramverket vara ett bra alternativ.  Om ni är, eller vill bli, leverantör till Försvarsmakten är KSF ett måste. Följer er marknad ett specifikt ramverk kan det vara bra att göra samma.

## Slutsats

Det viktigaste är att förstå att implementera ett ramverk kräver en ansträngning från alla nivåer i er organisation. Ledningen måste skapa och anpassa policys, samt se till att följa dom. Icke-teknisk personal måste förstå och följa dom, samt IT-personal måste implementera nya säkerhetsåtgärder för att uppfylla kraven. Detta är alltså inget man kan se som ett temporärt uppdrag, eller något man kan delegera bort. Det är en ny riktning för er organisation.

Det finns många populära ramverk. I det initiala skedet kan det vara komplicerat att bestämma vilket ramverk passar ert företag bäst. Genom att grundläggande undersöka vilka resurser, ambitioner och externa krav ert företag har så kan ni komma fram till vad som passar just er bäst, och förbereda för att implementera det.

Känns det fortfarande som en stor utmaning med stor komplexitet? IP Solutions har kunskapen och kapaciteten att hjälpa er med en implementation.

Vi kan hjälpa er att genomföra en GAP-analys (översikt på vad som saknas för en implementation), utveckla säkra funktioner och infrastruktur, pen-testning, sårbarhetshantering med mera. Skriv så kontaktar vi er om hur vi kan hjälpa just ert företag.

## Källor


CIS Controls - https://www.cisecurity.org/controls/v8

ISO27002 - https://www.iso.org/standard/75652.html

NIST CF – https://www.nist.gov/cyberframework

NIST SP-800-40 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

PCI-DSS - https://www.pcisecuritystandards.org/

KSF - https://isd.fmv.se/history/Sidor/FM-MUST-KSF.aspx