Thomas Verner

Styrning av verksamhetens IT

thomas.verner@isaca.se

ISACA Sweden Chapter

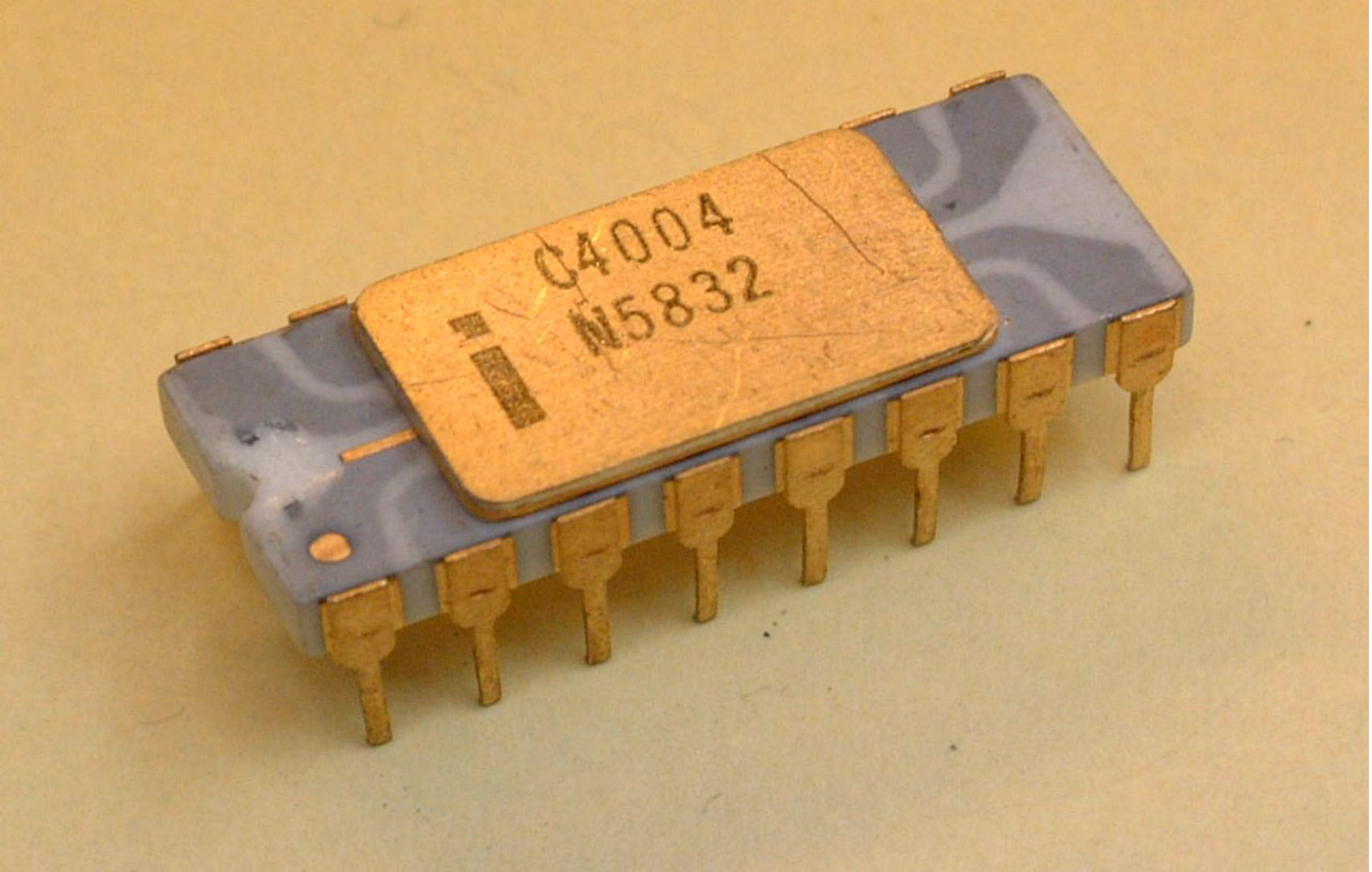
IIA Sweden

Session Agenda

- Some examples from my experiences
- Engagements
- Introduction to the publication
- A few of my governance obsessions and key messages

ISACA Sweden Chapter

IIA Sweden



ISACA Sweden Chapter

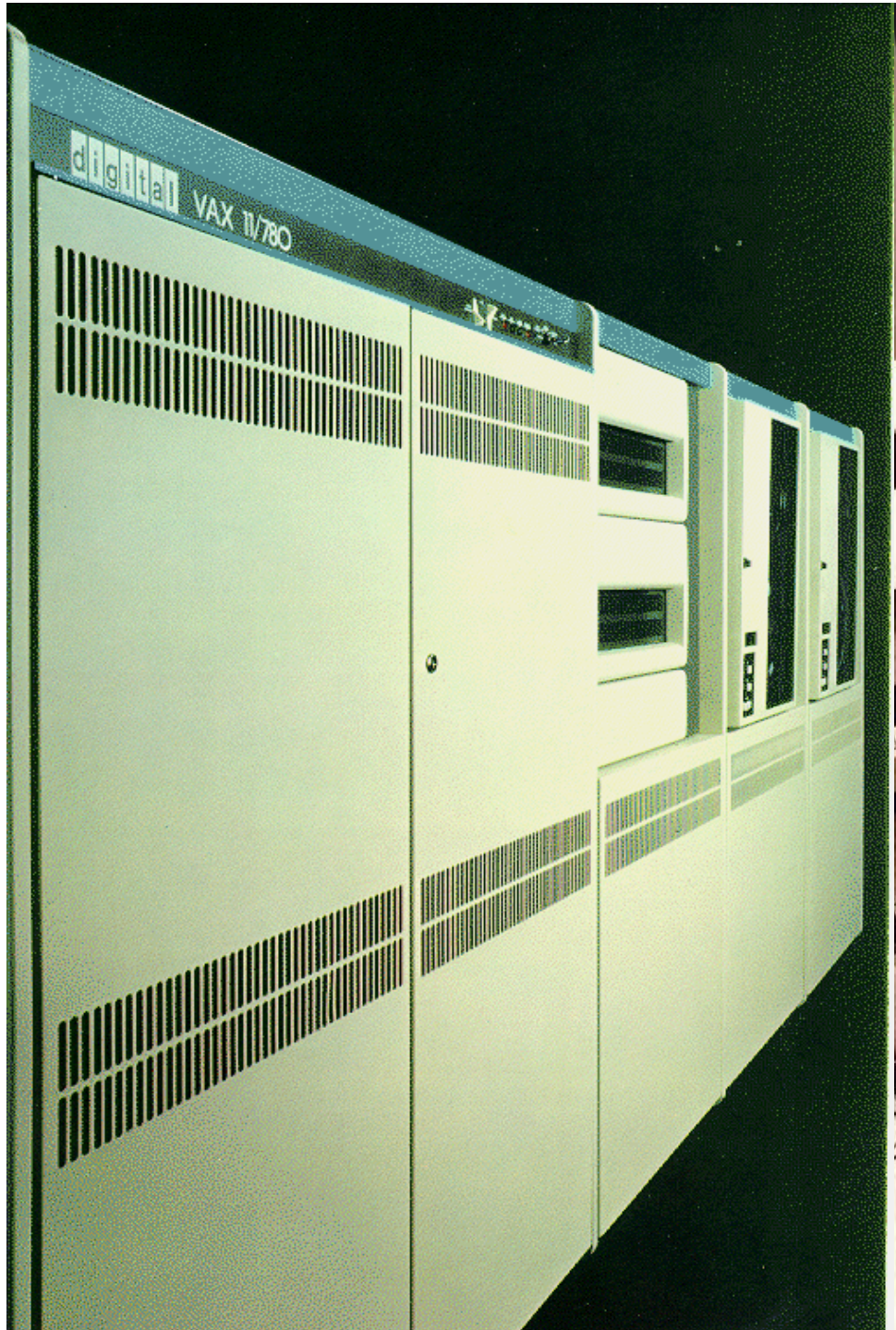
IIA Sweden

ISACA Sweden Chapter

IIA Sweden

ISACA Sweden Chapter

IIA Sweden



ISACA Sweden Chapter

IIA Sweden

ISACA Sweden Chapter

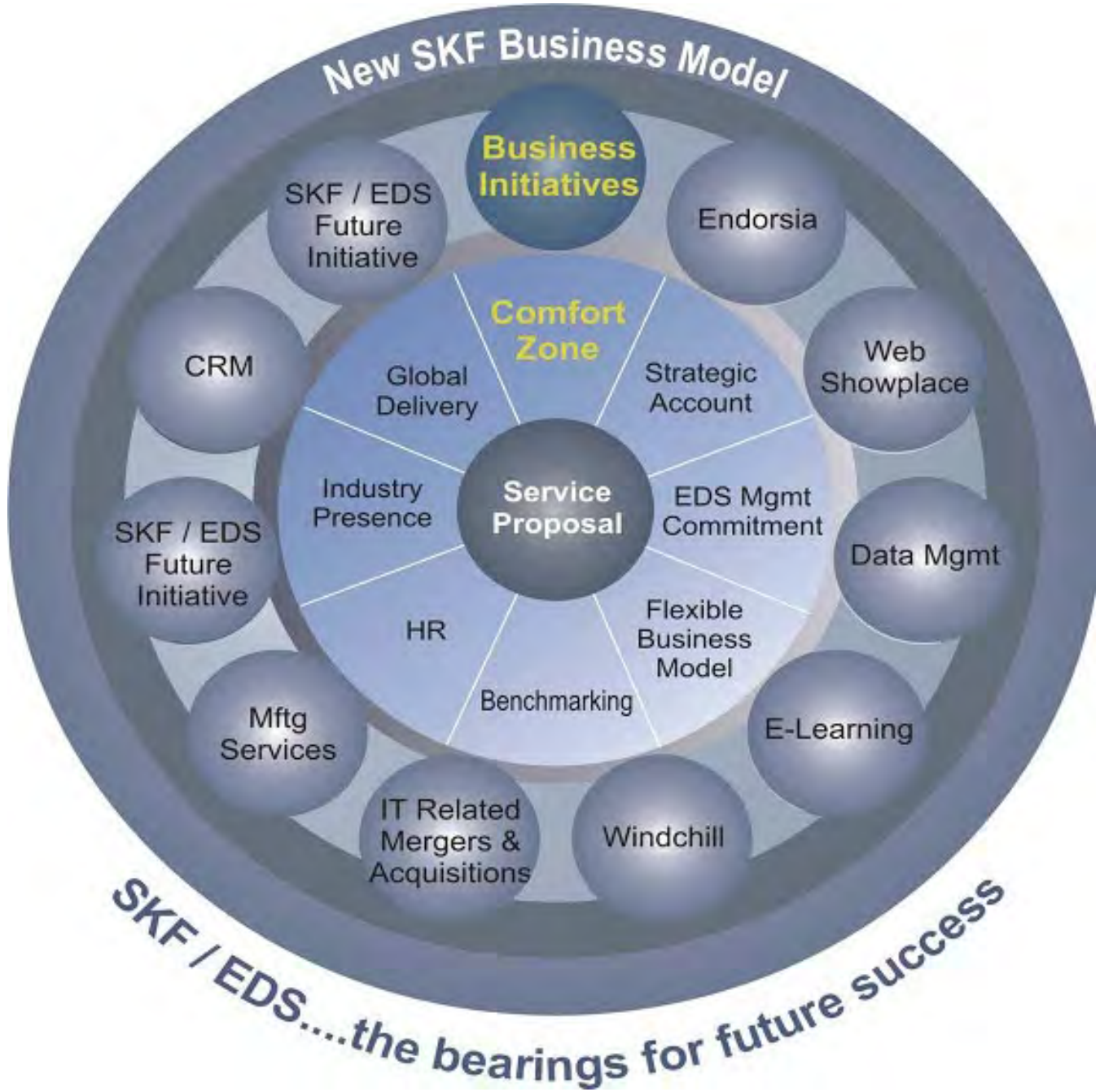
IIA Sweden

ISACA Sweden Chapter

IIA Sweden

ISACA Sweden Chapter

IIA Sweden



ISACA Sweden Chapter

IIA Sweden


pharmadule®
The power of certainty


Göteborgs
Stad


VOLVOFINANS


AkzoNobel
Tomorrow's Answers Today


Landstinget
Halland


VOLVO

GP


SANDVIK
Coromant


Nobel
Biocare


The Swedish Club


DN.


Elanders
Infomedia i praktiken.


benzler


plusenergi


Lyckeby


WirelessCar


Bostads
bolaget


COWI


BOXER
DIGITAL-TV MED EN VANLIG ANTENN.


SYDSVENSKAN


ISACA
Sweden Chapter


IIA
Sweden


Adwise
CONSULTING


STYRELSE
AKADEMIEN


DATAFÖRENINGEN
75
1949-2024


ISACA
Sweden Chapter


ISACA
Sweden Chapter


IIA
Sweden

Styrning av verksamhetens IT

En publikation framtagen av ISACA och IIA i samverkan

ISACA Sweden Chapter

IIA Sweden

Thomas Verner
thomas@verner.se

Om detta dokument

Denna vägledning är resultatet av ett initiativ taget av ISACA Sweden och IIA Sweden.

ISACA Sweden Chapter är en del av den internationella branschorganisationen **Information Systems Audit and Control Association** (ISACA).
ISACA har cirka 780 medlemmar i Sverige och över 180 000 globalt. Organisationen arbetar med verksamhets- och IT-ledare för att maximera värde och styra risker med fokus på information och teknologi.
ISACA grundades 1969 och är en non-profit medlemsorganisation som stödjer specialister inom områdena informationssäkerhet, cyber- säkerhet, IT-revision, riskhantering och styrning.

Internrevisorerna är en del av den internationella branschorganisationen **The Institute of Internal Auditors** (IIA). IIA Sweden har cirka 750 medlemmar i Sverige och över 235 000 globalt. Organisationen arbetar med internrevision, internkontroll, IT-revision, utbildning och säkerhet.
IIA grundades 1941 och är en non-profit medlemsorganisation som verkar för att stödja professionen och kompetensutveckla Sveriges internrevisorer.

ISACA Sweden Chapter

IIA Sweden

Varför har vi tagit fram denna publikation?

IT utgör en allt större del av vår tillvaro och därför också av våra organisationers funktioner och erbjudanden. Många verksamheter är direkt beroende av en effektiv och väl fungerande IT-miljö. Det är styrelsens och ledningens ansvar att tillse att organisationens IT-resurser används kostnadseffektivt och bidrar till verksamhetens mål, samt att kontinuerligt förutse och hantera risker, resursslöseri och brister för att inte äventyra verksamheten.

Ett stort beroende av en väl fungerande IT-miljö

Brister i IT-kontroller kan ha stor påverkan på en organisations produktivitet, finansiella situation och anseende. Det är av stor vikt att styrelsen, liksom i andra affärskritiska frågor, åtar sig en väl definierad styrande och strategisk roll utan att inkräkta på ansvar av taktisk och operativ karaktär.

Brister i IT-kontroller kan ha stor påverkan på en organisations produktivitet, finansiella situation och anseende

ISACA Sweden Chapter

IIA Sweden

Vem vänder vi oss till med denna publikation?

Vägledningen vänder sig till styrelseledamöter i alla sorters verksamheter inom privat eller publik sektor, med tonvikt på mindre och medelstora organisationer som saknar stöd av specialister för att analysera och bereda underlag för styrelsebeslut.

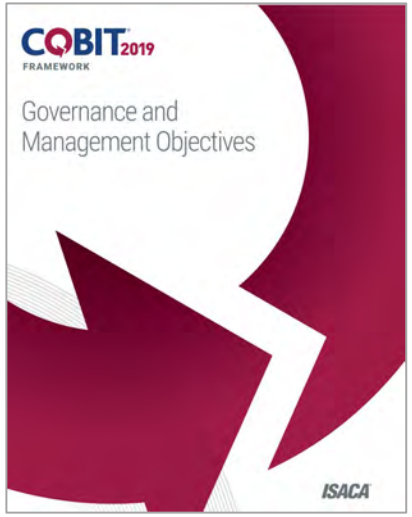
ISACA Sweden Chapter

IIA Sweden

Inspiration till publikationen

Rekommendationer som föreslås i vägledningen utgår från ramverk och råd som har utvecklats av IIA och ISACA på global nivå. Dessa råd har översatts med hänsyn tagen till de förutsättningar som är relevanta för Sverige. Även andra publikationer, som etablerade industristandarder och rekommendationer för att hantera IT med god kontroll, har beaktats.

Som inspiration kan vi bl.a. nämna Aktiebolagslagen, Svensk kod för bolagsstyrning, Vägledning till god styrelsesed, COBIT, IT-checklista för styrelser, ECODA Cyber-Risk Oversight



ISACA Sweden Chapter

IIA Sweden

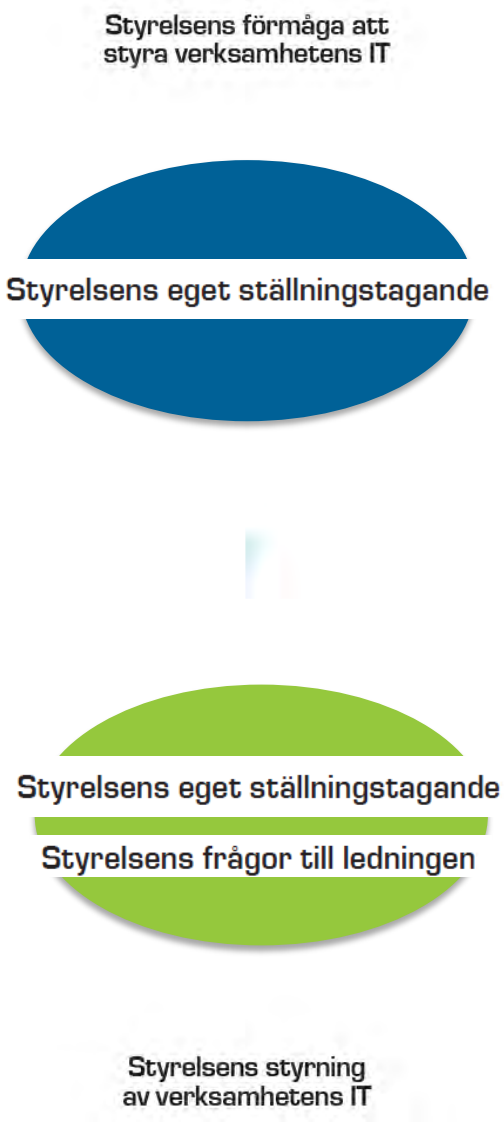
Styrning från det strategiska till det operativa

Vi har identifierat två huvudområden för styrelsearbetet:

1. Styrelsens förmåga att styra verksamhetens IT
2. Styrelsens styrning av verksamhetens IT

När det gäller förmåga bör styrelsen göra sina egna ställningstaganden

När det gäller styrningen bör styrelse göra sina egna ställningstaganden men även ställa frågor till ledningen



ISACA Sweden Chapter

IIA Sweden

Styrning från det strategiska till det operativa

Vi har identifierat sju områden som avser styrelsens förmåga att styra verksamhetens IT samt sju områden som avser styrelsens styrning av verksamhetens IT.

Det finns relationer mellan flera av dessa områden som är lite tydligare vilket vi har lyft fram med pilar.

Med utgångspunkt från svenska förhållanden har vi identifierat att styrningen utgår från gällande lagstiftning och regulatoriska krav som bestämmer ton, omfattning och inriktning för styrelsearbetet, vilket drivs mot att de resurser som används skapar efterfrågat värde.

ISACA Sweden Chapter

IIA Sweden

Styrning från det strategiska till det operativa

Övergripande beskrivning med reflektioner för det område som berörs

Checklista för att stämma av att ställningstagande har beaktats

Öppna frågor istället för frågor som besvaras med Ja eller Nej

ISACA Sweden Chapter

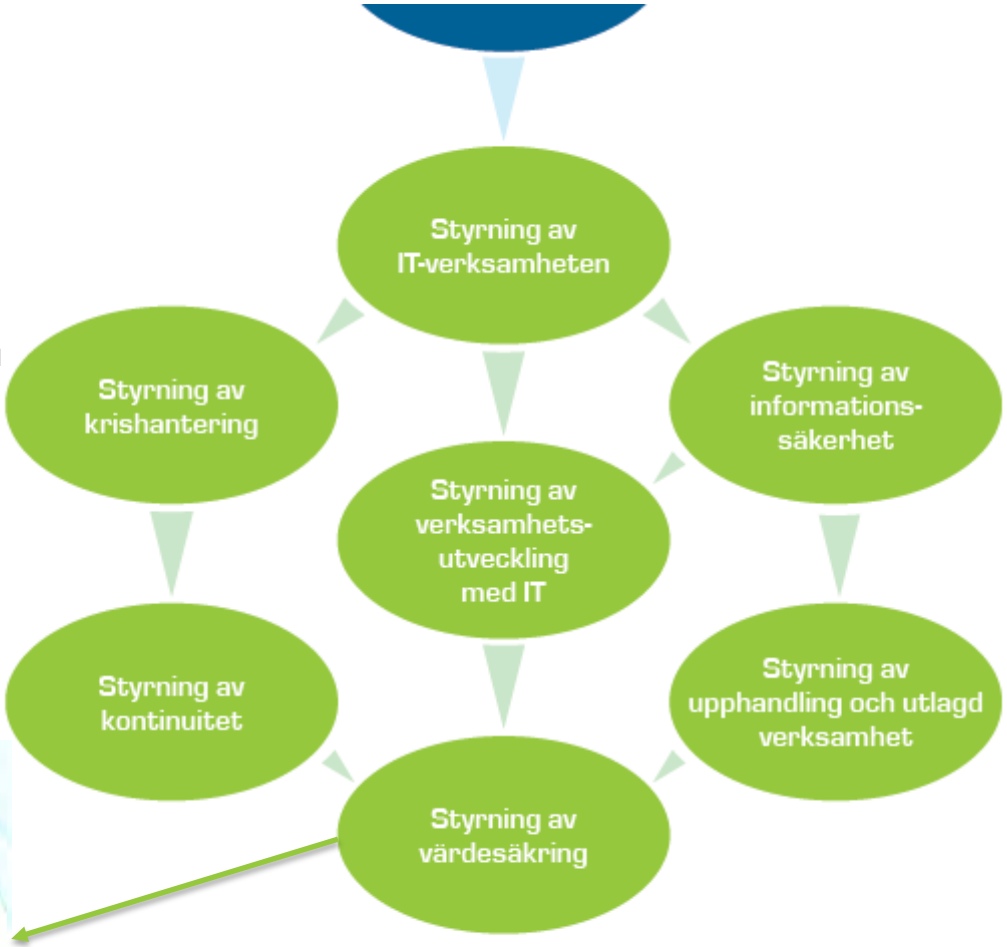
IIA Sweden

Styrning från det strategiska till det operativa

Öppna frågor istället för frågor som besvaras med Ja eller Nej

Checklista för att stämma av att ställningstagande samt frågor till ledningen har beaktats

Övergripande beskrivning med reflektioner för det område som berörs



Styrelsens styrning av verksamhetens IT

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Käpphäst - något som man är mycket intresserad av, ständigt och gärna sysselsätter sig med eller återkommer till…

“Passion and favorite themes”

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Styrning, ledning och ansvar

- Styrelsen skall inta en väl definierad styrande strategisk roll utan att inkräkta på ansvar av taktisk och operativ karaktär

- Har styrelsen egen kompetens och/eller har man säkrat tillgång till oberoende kompetens för att kunna bedöma verksamhetens IT, informationssäkerhet och cybersäkerhet?

- Om en IT-tjänst läggs på en extern part, så kvarstår ansvaret hos organisationen och därmed styrelsen. Outsourcingavtal har dessutom oftast en ansvarsbegränsning som inte motsvarar köparens risk

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

IT är ingen separat verklighet

- Generellt är det ingen skillnad på verksamhetens IT och andra affärskritiska resurser

- Hur har styrelsen identifierat de IT relaterade förutsättningar som är nödvändiga att etablera för att bedriva verksamheten?

- På vilket sätt behöver bolagsordning och ägardirektiv förändras?
- I vilken mån behöver styrelsens arbetsordning kompletteras?
- Hur behöver instruktionen för verkställande ledning kompletteras?
- I vilken mån behöver rapporteringsinstruktionen kompletteras?

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Verksamhetsutveckling

- Hur har ledningen säkrat tillräckliga verksamhetsresurser för genomförandet?

- Hur är kvaliteten på den information/det befintliga data som ska föras över till, och användas av, det nya systemet?

- I de fall utvecklingen drivs som projekt bör styrelsen vara medveten om att en styrgrupp på eget initiativ sällan stoppar projekt
(… The planning fallacy …)

- Har styrelsen säkrat extern och oberoende revision av pågående projekt?

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Informationssäkerhet

- Informationssäkerhet är inte en fråga enbart för IT-verksamheten
  Den ska beaktas ur samtliga verksamhetsperspektiv

- Vilken är den skyddsvärda informationen i organisationen (produktinformatıon, recept, persondata etc.) - verksamhetens ”kronjuvel(er)”

- Vilken är den information som en eller flera externa tjänsteleverantörer inte får hantera eller ha åtkomst till?

- Håll tekniskt isär olika verksamheter där det är möjligt. IT i industrimiljö kan fungera som ingång/bakdörr till administrativa system vid en cyberattack

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Förbereda krishantering

- Vilka lagar och regulatoriska krav måste efterlevas och som eventuellt kan förändras inom en nära framtid? (t.ex EU-direktivet NIS2)

En sammanfattning av NIS2

- NIS2 är en uppdatering av det tidigare NIS-direktivet och syftar till att stärka skyddet för samhällsviktiga tjänster genom att säkerställa informationssäkerhet i hela EU.
- Planeras att bli **svensk lag** under hösten 2024
- **Alla organisationer** som är involverade i **samhällsviktiga tjänster**, oavsett om de är offentliga eller privata, omfattas av direktivet.
- Organisationer som omfattas av NIS2 **måste vidta lämpliga tekniska och organisatoriska åtgärder** för att säkerställa informationssäkerheten.
- De måste **rapportera allvarliga incidenter** till myndigheterna och samarbeta med andra organisationer för att hantera incidenter som påverkar samhällsviktiga tjänster.
- NIS2 innebär även skärpta tillsynsåtgärder och företag som inte följer standarderna riskerar **betydande böter**. Styrande organ kan även hållas **personligt ansvariga** om inte lagstiftningen efterlevs.

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Förbereda krishantering

- Vilka lagar och regulatoriska krav måste efterlevas och som eventuellt kan förändras inom en nära framtid? (t.ex EU-direktivet NIS2)

- En väl hanterad kris kan stärka verksamhetens varumärke (Kalix kommun) medan en sämre hanterad kris skadar det

- Det är viktigt att kombinera och harmonisera hantering av IT-kriser med andra typer av beredskap och krisplaner

- Styrelsen måste tillse att ett tydligt mandat ges till ansvariga inom verksamhetens IT för att de skall kunna agera operativt och skyndsamt vid en kris

ISACA Sweden Chapter

IIA Sweden

Några av mina käpphästar

Kontinuitetshantering

- Hur har ledning och verksamhet förberett sig för att vidmakthålla en verksamhet som kan accepteras av våra kunder/intressenter i väntan på att IT-systemen kan återställas?

- Vad är resultatet av tester av kontinuitetsplaner där vi både verifierar att de fungerar och övar att använda dem för att säkerställa att de är ändamålsenliga och effektiva?

- Återställande av verksamheten (IT-system): Hur ser den utarbetade prioriteringsordningen ut?

ISACA Sweden Chapter

IIA Sweden

Styrning av verksamhetens IT

En publikation framtagen av ISACA och IIA i samverkan

ISACA Sweden Chapter

IIA Sweden

Thomas Verner
thomas@verner.se
0705 769200