Styrning av verksamhetens IT

Stöd för styrelsens arbete med IT och informationssäkerhet

Version: (2024)

Introduktion

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.

Den här vägledningen är framtagen av IIA Sweden och ISACA Sweden för att hjälpa styrelser med en allmän orientering och stöd i generella IT-relaterade frågor.

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.

Som underlag till vägledningen har ett antal områden som kan vara relevanta för styrning av verksamhetens IT valts ut (se illustration). Urvalet är baserat på vår uppfattning om vanligt förekommande riskområden. 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.

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.

Styrelsens förmåga att styra verksamhetens IT

Styrelsens styrning av verksamhetens IT

Kontext

Styrningen ska fokusera på att hantera resurser och risker. Den ska också beakta andra aspekter, till exempel effektivisering, för att åstadkomma värdesäkring, samhällsnytta och hållbarhet.

I den privata sektorn är det Aktiebolagslagen och Svensk kod för bolagsstyrning som reglerar styrelsens ansvar. I den offentliga sektorn gäller en samling av förordningar. Det finns även organisationsformer, till exempel stiftelser, som drivs utifrån stadgar där styrelsens ansvar är definierat.

Del av styrelsens arbete är att utvärdera lagstiftning och regulatoriska krav, då dessa ställer grundläggande krav på hur verksamheten ska hantera information och IT.

När denna vägledning berör begreppet informationssäkerhet kan det ses som ett paraplybegrepp för IT-säkerhet och cybersäkerhet samt i viss utsträckning dataskydd. För dessa begrepp är Informationsteknologi (IT) en gemensam nämnare som berör ett stort antal frågeställningar.

IT omfattar både befintliga IT-lösningar och initiativ till ökad digitalisering, till exempel som del av verksamhetsutvecklingen. IT kan utgöra såväl administrativt stöd som en väsentlig del av verksamhetens leverans. Ökad användning av IT i fabriker och produktionsprocesser (OT), med en tilltagande integration mellan administrativa och industriella system som följd, ställer högre krav på informationssäkerhet. Styrelsen bör säkerställa att olika områden hålls isär där det är möjligt, då IT i industrimiljö kan fungera som ingång till administrativa system vid en cyberattack.

Vi har valt att inte lyfta fram specifika tillämpningar av IT eller OT, för att hålla vägledningen på en övergripande nivå. Vägledningen ger ej heller någon fördjupning i etiska aspekter eller hållbarhet.

När det gäller den operativa ledningen i en verksamhet avser detta verkställande direktör (VD), generaldirektör (GD) eller liknande roll. Vi har valt att beskriva detta som ”verkställande ledning”.

Lagstiftning och regulatoriska krav

Inom styrelsen är det nödvändigt att ha en tydlig bild av vilka lagar och regelverk som berör verksamhetens IT. Notera att vissa regelverk ställer krav på personligt ansvar vid brister i efterlevnad. Det kan vara värdefullt att ha tillgång till legal expertis för att tolka dessa krav. Styrelsen bör säkerställa att även ledningen har tillgång till samma expertis.

Styrelsen ska också säkerställa att ledningen tillser att personal som arbetar med verksamhetens IT är insatt i gällande lagar och regulatoriska krav. Detta ska ske fortlöpande så att verksamheten kontinuerligt anpassas till eventuella förändringar i kraven.

Brister i efterlevnad kan innebära att förtroendet för verksamheten äventyras vilket i sin tur kan påverka bland annat efterfrågan, försäljning och förmåga att attrahera kompetent personal.

Styrelsens eget ställningstagande:

- Hur har vi utvärderat vilka lagar och regulatoriska krav som måste efterlevas och som eventuellt kan förändras inom en nära framtid?
- Vilken kompetens och förmåga har ledningen när det handlar om att kommunicera de krav på efterlevnad som gäller?

Styrelsens strategiska stöd från GRC-funktioner

En balanserad syn på verksamheten, baserad på en realistisk bedömning av de beslut som fattas, åstadkoms genom att kombinera styrning, risk och efterlevnad. De tre delarna samlas i begreppet GRC (governance, risk och compliance), där kompetensen inom dessa områden samverkar.

Genom att förstå, värdera och hantera de risker som är naturliga för verksamheten, skapas en bredare bas för styrelsens beslut samt förutsättningar för att genomlysa enskilda frågor på djupet. Detta omfattar även att agera enligt lagar och regulatoriska krav och möta intressenternas förväntningar.

Större eller reglerade organisationer kan ha en internrevisionsfunktion. Internrevisionsfunktionen är ett bra och oberoende verktyg som ger styrelsen insikt i verksamhetens interna styrning, kontroll och riskhantering. Styrelsen bör säkerställa att relevanta IT-relaterade riskområden finns med i internrevisionens revisionsplan samt att internrevisionen har nödvändig kompetens för att utvärdera hantering av dessa risker.

Det strategiska stödet från GRC-funktionen ger ett holistiskt perspektiv som möjliggör för styrelsen att bedöma risker och resurser i relation till verksamhetsnytta och affärsnytta.

GRC tillför bland annat:

1. Djupare och mer balanserat beslutsfattande genom tillgång till rätt information vid rätt tidpunkt, för rätt mål och rätt kontroller.
2. Genomarbetade underlag till beslut som kan ifrågasätta eller bekräfta information.
3. Effektivt arbete med att förstå och agera på risker.

Styrelsens eget ställningstagande:

- Hur säkerställer vi att vi får ett tillräckligt bra beslutsunderlag?
- I vilken mån får vi en samlad bild över de risker som finns inom organisationen och hur väl de hanteras?
- På vilket sätt vinner styrelsearbetet på att ha en implementerad GRC-strategi?

Riskvillighet

Styrelsen ska formulera en strategi som beskriver de risker verksamheten är beredd att ta, hur riskerna mäts samt relevanta nyckeltal. För att sätta ramarna för verksamheten ska styrelsen definiera vilka risker IT medför samt beskriva hur stor risk som är acceptabel. I vissa sammanhang benämns detta som riskaptit eller risktolerans. Det kan handla om att bestämma graden av tillgänglighet till digitala tjänster, att bestämma vilken balans mellan olika prioriteringar som krävs för att kunna bearbeta informationsmängder eller att fatta beslut om i vilken utsträckning information och IT-tillgångar ska skyddas. Även risker relaterade till lagar och regulatoriska krav ska beaktas i de fall brister kan få stor påverkan på bolaget.

Med utgångspunkt i riskvilligheten ska styrelsen bedöma det övergripande behovet av resurser för IT samt utvärdera att resurserna ger önskad avkastning. Att försäkra sig om att det finns rätt resurser vid rätt tillfälle är en avvägning som kan medföra ytterligare investeringar.

Utöver de risker som är kända bör styrelsen även ta ställning till hur verksamheten ska agera i samband med framtida risker som är okända vid analystillfället. En ny verklighet kan utvecklas på kort tid.

Riskanalyser av god kvalitet är viktiga för att kunna fatta bra beslut. Det innebär att verksamheten måste förlita sig på experter för att ta fram och utvärdera riskerna. Här är det av största vikt att styrelsen granskar experternas insatser för att säkerställa att de agerar för verksamhetens bästa och inte i egenintresse.

Styrelsens eget ställningstagande:

- På vilket sätt har vi vägt möjligheter med ett större risktagande mot kostnader för risker i en riskstrategi?
- Vilka resurser är nödvändiga för att genomföra verksamhetsstrategin, och vilka risker föreligger för dessa resurser?
- Hur går vi tillväga för att tydligt utvärdera att vi har använt våra resurser på ett förnuftigt sätt?
- I vilken utsträckning har styrelsen kompetens för att kunna bedöma verksamhetens IT, informationssäkerhet och cybersäkerhet?

Styrelsens roll i IT-frågor

Generellt är det ingen skillnad på verksamhetens IT och andra resurser, oberoende av vilken verksamhet som bedrivs. Dock har verksamhetens IT stor påverkan på möjligheterna att bedriva verksamheten effektivt och med hanterad risk. Verkställande ledning sköter riskbedömningar, med styrelsen som stöd. Styrelsen ska säkerställa att ledningen har kompetens att kunna fatta beslut i IT-frågor och göra relevanta riskbedömningar.

Det är likaså styrelsens uppgift att fastställa verksamhetens övergripande mål och strategi – och då även för verksamhetens IT. I arbetet med målsättningarna ska risker och beroenden relaterade till all IT beaktas, inkluderat administration, produktion samt eventuell IT i produkter och tjänster. Det är nödvändigt att styrelsen har denna förståelse för att kunna ge rätt styrning, bedöma risker och säkerställa att återkopplingen från verksamheten stödjer styrelsearbetet.

En intressentanalys ska finnas på plats som stöd för styrelsens arbete. Intressenterna kan se olika ut i olika verksamheter och utgöras av förslagsvis kunder, samarbetspartners, leverantörer, konsulter, medarbetare, kommuner, lokalsamhälle, branschorganisationer med flera.

Sammanfattningsvis innebär styrningen att:

1. Intressenternas behov, villkor och alternativ utvärderas för att komma överens om de mål som styrelsen definierar.
2. Direktiv för ledningen fastställs.
3. Resultat och efterlevnad återrapporteras till styrelsen i relation till överenskomna direktiv och mål.

Styrelsens eget ställningstagande:

- Hur har styrelsen identifierat de förutsättningar som är nödvändiga att etablera för att bedriva verksamheten?
- På vilket sätt kan IT bidra till värdesäkring, och vilka resurser behöver beaktas av ledningen för att uppnå verksamhetsmålen?

Mätning och rapportering

En central del av styrningen är att etablera mätetal och KPI:er för att följa upp att IT-verksamheten bedrivs i enlighet med verksamhetens affärs- och IT-strategi. Ledningen gör uppföljningar löpande, medan styrelsen gör mer periodiska uppföljningar. Styrelsen ställer krav på vad som ska mätas och hur det ska rapporteras. Styrelsen förväntas också ha klart för sig hur resultaten ska användas i styrelsearbetet.

Det är nödvändigt att avvikelser från mätetal och KPI:er rapporteras tydligt, och att åtgärdsplaner etableras för att följa och redovisa utvecklingen mot etablerade mätetal och KPI:er. Mätetalen ska följa alla delar av IT-verksamheten, exempelvis automatisering/digitalisering, resursoptimering, verksamhetsutveckling och riskvillighet avseende informations- och cybersäkerhet.

Styrelsens eget ställningstagande:

- Hur kan vi säkerställa att mätetalen är förankrade och implementerade i bolagets operativa ledning?
- I vilken utsträckning kan vi vara säkra på att mätetalen är ändamålsenliga och att nivåerna är riskavägda?
- På vilket sätt har vi säkerställt tillräcklig transparens i mätetalen för att kunna styra utifrån utfallet och utveckla mätetalen?

Resursoptimering

Genom att optimera resurser för verksamhetens IT avseende personal, processer, IT-lösningar och samarbetspartners, bidrar dessa tillsammans till att uppfylla verksamhetsmål. Optimeringen är ledningens ansvar, men styrelsen behöver vara delaktig i principbeslut och styra den strategiska inriktningen.

Resursoptimering kan handla om att framtidssäkra resurser, till exempel utveckla och behålla nyckelkompetens, eller att balansera resurser mellan ny funktionalitet och befintlig funktionalitet. Det kan också handla om att kontinuerligt investera i utveckling av de IT-lösningar som är en förutsättning för att bedriva verksamheten, i syfte att bibehålla konkurrenskraft. Även processer måste utvecklas och anpassas för att vara relevanta vid varje enskilt tillfälle.

Resursoptimering innebär också att värdera resurser för att kunna fatta beslut om prioriteringar. Genom en holistisk syn på resursbehov kan styrelsen undvika silobeteende och subjektiva bedömningar som riskerar att snedvrida resursfördelningen.

Styrelsens eget ställningstagande:

- Hur säkerställer vi att styrelsen har rätt underlag för att utvärdera behov av resurser och för att kunna fatta principbeslut?
- Vilka beslut har vi förmåga att fatta när det gäller att balansera resurser vi har tillgång till och resurser vi har behov av?
- På vilket sätt kan vi utvärdera om resursfördelningen är optimal?

Ansvar för styrning av IT-verksamheten

I Aktiebolagslagen och Svensk kod för bolagsstyrning framgår styrelsens ansvar. I relation till IT ansvarar styrelsen för att säkerställa styrning av digitalisering, IT-system och relaterade processer, en robust behörighetshantering, efterlevnad av lagkrav samt en balanserad hantering av risker.

Risker kan vara av operativ natur (till exempel en störning av verksamheten) eller varumärkesrisker (till exempel otillförlitlig informationsgivning och läckage av data).

Styrelsen ska säkerställa att det finns relevant kompetens för att kunna driva IT-verksamheten.

För offentlig verksamhet regleras motsvarande krav i förordningar samt kommunallagen.

Som styrelseledamot ska du bidra till att etablera en god IT-styrning bestående av fem huvudsakliga komponenter:

1. En stark koppling av IT till affärsstrategin/verksamhetsstrategin.
2. Ett systematiskt arbete för att säkra värdet av IT-investeringar och initiativ.
3. Ett aktivt arbete med att vårda IT-tillgångarna (människor, data /information, utrustning/licenser, system, processer och pengar).
4. En aktiv hantering av risker (till exempel informationssäkerhet, införandeprojekt och tillgänglighet till information och system).
5. Kontinuerlig utvärdering för att säkerställa att IT-verksamheten stödjer verksamheten

Styrelsens eget ställningstagande:

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

Styrning av IT-verksamheten

IT-strategin ger stöd för ledningens planering och prioritering av verksamhetens IT. Styrelsen sätter ramar och inriktning baserat på den övergripande verksamhetsstrategin. Styrelsearbetet bör definiera dessa ramar i relation till omvärld, geopolitiska förändringar, konkurrenssituation och teknisk utveckling, baserat på relevant information från ledningen.

Tidshorisonten bör vara långsiktig men också pragmatiskt tillämpad så att det finns möjlighet att reagera på betydande omvärldshändelser som påverkar verksamhetens IT. Styrelsen ska säkerställa att IT-strategin stämmer överens med övriga strategiska frågor. Strategin ska också utgå från riskvillighet samt innehålla mätbara element som kan rapporteras till styrelsen.

Att ta fram en IT-strategi innebär en balansgång där styrelsen dels behöver beakta hur verksamhetens IT kan bidra till ökad effektivitet och konkurrenskraft, dels bedöma intryck från omvärld och andra organisationer utifrån relevans och värde för den egna verksamheten.

Styrelsens eget ställningstagande:

- Hur kan vi få relevant återkoppling på att risker har beaktats samt att resurser används på effektivt och ändamålsenligt sätt?
- Vilket behov har vi av en extern utvärdering för att få en rättvisande bild?
- På vilket sätt kan styrelsen förbereda sig och hantera avvikelser?

Styrelsens frågor till ledningen:

- Hur har IT-strategin harmoniserats med övergripande verksamhetsstrategi och styrning?
- Hur säkras förutsättningar och tillräckligt med resurser i personal som både har IT-kompetens och annan relevant kompetens.
- Hur säkras resurser i IT-lösningar för att kunna genomföra IT-strategin utifrån givna prioriteringar?
- Hur är strategin balanserad, utmanande eller återhållsam?
- Hur säkerställer ledningen att styrelsen får relevant och användbar rapportering?

Styrning av krishantering

En väl hanterad kris kan stärka verksamhetens varumärke, medan en sämre hanterad kris kan skada detsamma.

Den övergripande förmågan att agera vid kriser påverkas till stor del av hur väl verksamhetens IT kan stå emot påfrestningar och anpassas till nya och oplanerade situationer. I förlängningen handlar det även om integrering i samhällets krigsberedskap.

Det kan ge betydande synergieffekter att kombinera och harmonisera krishanteringen med andra typer av beredskap, till exempel hur verksamheten hanterar händelser som brand eller när medarbetare skadas eller saknas i tjänst.

Styrelsen måste ha beredskap för hur verksamheten ska agera vid dessa händelser och ha en tydlig bild av hur arbetet ska bedrivas under den begränsade tidsperiod som verksamheten är i kris. Genom att arbeta fram en strategi som tar hänsyn till olika typer av kriser, minimeras den tid det tar att agera. Strategin måste också ta ställning till det digitala beroendet så att styrelsen ger ett tydligt, eget mandat till ansvariga inom verksamhetens IT att agera operativt och skyndsamt vid kris. Det kan till exempel handla om att stänga ner hela eller delar av den digitala infrastrukturen i samband med ett cyberangrepp, även om det innebär att verksamheten stoppas.

Styrelsens eget ställningstagande:

- På vilket sätt stödjer kommunikationsstrategin styrelsens agerande i händelse av en kris?
- Vilken kommunikation med externa parter och medarbetare i verksamheten omfattas?

Styrelsens frågor till ledningen:

- Hur hanteras kriser relaterade till verksamhetens IT?
- Hur har grundläggande rutiner som används för andra krissituationer inkluderats?
- Hur har ledningen resonerat kring prioriteringsordningen för att stänga ner eller återställa system och IT-stöd?
- På vilket sätt har ledningen gett mandat till IT-organisationen att agera snabbt vid händelser som kan skada verksamheten, till exempel vid cyberangrepp?

Styrning av informations-säkerhet

Informationssäkerhet är inte en fråga enbart för IT-verksamheten utan ska beaktas ur såväl samtliga IT-perspektiv (administration, produktion, produkter och tjänster) som ur verksamhetsperspektiv, speciellt när det gäller digitaliserade verksamhets- och affärsprocesser.

Det är viktigt att styrelsen etablerar och underhåller ett ledningssystem för informationssäkerhet (LIS) där informationstillgångar bedöms och hanteras på ett strukturerat sätt, utifrån verksamhetens behov. Ledningssystemet ska omfatta en rapportering inför ledningen, minst en gång per år. Även styrelsen bör begära en egen föredragning som underlag för att kunna ge bra direktiv och få relevant återkoppling. Styrning av informationssäkerhet har även en direkt påverkan på verksamhetens dataskyddsarbete enligt exempelvis dataskyddsförordningen (GDPR). Det finns även annan skyddsvärd information i organisationen (produktinformation, recept etc.) som har en direkt påverkan på verksamhetens förmåga att nå sina mål, och på verksamhetens ”kronjuvel(er)”.

Styrelsens eget ställningstagande:

- Hur arbetar verksamheten med ledningssystem för informationssäkerhet?
- Hur har vi beaktat risker avseende informationssäkerhet för att uppnå våra överenskomna mål?
- I vilken utsträckning har det säkerställts att styrelsen får information om brister i informationssäkerhet samt det skydd verksamheten har fått?
- Hur säkerställer ledningen att arbetet är systematiskt och långsiktigt, samt bedömer vilka effektmål som kan ställas och följas upp?

Styrelsens frågor till ledningen:

- På vilket sätt skyddas verksamhetens viktigaste tillgångar, dvs. ”kronjuvel(er)”?
- Hur ser utfallet ut av ledningens genomgång avseende informationssäkerhet?
- Vilka kostnader driver risker relaterade till informationssäkerhet?
- Vad är vi mest sårbara för när det gäller externa respektive interna hot?
- Om det finns ett uttalat stöd för att arbeta systematiskt med informationssäkerhet, hur driver ledningen dessa frågor?

Styrning av verksamhets-utveckling med IT

Styrelsen ska säkerställa att förutsättningar för effektivt och ändamålsenligt utvecklingsarbete finns på plats i form av rätt organisation och arbetssätt. Arbetssättet bör bland annat omfatta kriterier för val av utvecklingsinitiativ, fördelning av utvecklingsramen samt oberoende godkännande för avslut av utvecklingsinitiativ. Styrelsen ska också säkerställa att verksamhetsutvecklingen stämmer överens med verksamhetens strategiska inriktning samt fatta beslut om resursnivå för verksamhetsutveckling.

Styrelsen bör även kräva att verksamheten analyserar och hanterar risker som uppkommer i samband med verksamhetsutveckling. I de fall utvecklingen drivs som projekt bör styrelsen vara medveten om att en styrgrupp på eget initiativ sällan stoppar projekt. Ytterligare en utmaning som styrelsen kan behöva känna till är risk för bristande ledningskapacitet och mandat. I dessa fall kan styrelsen behöva ingripa för att hantera särskilt organisationsöverskridande projekt. Eskaleringsvägar måste också etableras så att styrelsen kan begära revision av projekt, till exempel av internrevisionen. Det kan också innebära överväganden där tempot i projekt behöver öka eller minska.

Vanliga misstag är till exempel att budget överskrids samt att utvecklingen drar ut på tiden med följdeffekten att lagstiftning som träder i kraft vid ett visst datum förbises. Styrelsen bör också vara observant på under- eller överinvesteringar. Kostnader underskattas ofta för att få planen för verksamhetsutvecklingen godkänd, men kan också överskattas i syfte att behålla medel man har haft tillgång till tidigare, vilket leder till resursslöseri.

Styrelsens eget ställningstagande:

- Hur har vi beaktat informationssäkerhet och andra lagar och regelverk som påverkar verksamhetsutvecklingen?
- Hur är kvaliteten på den information/befintlig data som ska föras över till, och användas av, det nya systemet?
- Hur har vi säkrat tillräckliga egna resurser för genomförandet?
- Hur har verksamheten gjorts medveten om att egna resurser behöver tillföras?
- På vilket sätt kan vi säkerställa att vi håller oss inom givna ramar där både tillägg och avgränsningar dokumenteras?

Styrelsens frågor till ledningen:

- Hur görs bedömningar för att ha tillräckliga egna resurser för genomförandet?
- Hur verifieras att verksamheten är medveten om att egna resurser behöver tillföras?
- Hur involveras externa oberoende parter för att utvärdera utvecklingsprojekt under projektets gång?
- Är planen för verksamhetsutveckling tydlig och tidsbegränsad?
- Har planen tydliga mätbara delmål inklusive rapportering om ekonomin?

Styrning av kontinuitet

Verksamheten beslutar vilka krav på tillgänglighet som ska gälla för IT-tjänster, och vad som är en tolerabel nivå vid händelse av ett avbrott eller en störning. Tillgängligheten omfattar tillgång till personal, försörjning av varor samt andra resurser som är nödvändiga för att kunna arbeta operativt. Brist på skydd av dessa tillgångar kan utnyttjas vid en attack. Inom vissa verksamhetsområden finns det även legala krav på tillgänglighet som måste beaktas.

Styrelsen kan bidra till en samsyn mellan verksamhetens organisatoriska delar och verksamhetens IT för att utarbeta alternativa arbetssätt i händelse av en störning som begränsar tillgången till IT. Behoven måste utgå från den verksamhet som bedrivs. Detta innefattar att verksamhetens IT får mandat att kortsiktigt göra väl avvägda avsteg från det normala ramverket för intern kontroll, för att snabbt vidta åtgärder som kan begränsa skada.

Tidsaspekter ska beaktas eftersom alternativa arbetssätt kan innebära betydande kostnader. Kontinuitetsplaneringen omfattar även hur en återgång till normal verksamhet kan hanteras effektivt, samt en plan för kommunikation.

Det är också nödvändigt att väga kostnader för lösningar som säkerställer hög kontinuitet mot kostnader som uppstår då en kontinuitetsplan sätts i verket.

Styrelsens eget ställningstagande:

- Hur har vi säkerställt att vi har gjort en tillräckligt bra analys för att kunna ta ställning till hur vi balanserar tillsatta IT-resurser och IT-risker i vår planering?
- Hur ska vi agera i händelse av att kontinuitetsplanen har aktiverats?

Styrelsens frågor till ledningen:

- Hur har ledning och verksamhet förberett sig för att vidmakthålla en verksamhet som kan accepteras av våra kunder/intressenter?
- 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?
- Vilka scenarier i kontinuitetsplanerna behöver styrelsen ta höjd för i sin riskhantering?
- Hur ser den utarbetade prioriteringsordningen för återställande av IT-system ut?

Styrning av upphandling och utlagd verksamhet

Organisationer använder sig ofta av externa leverantörer av IT-tjänster, exempelvis molntjänster och samarbetspartners. Det är viktigt att inköp och upphandling görs på ett sätt som säkerställer att dessa tjänster levererar prestanda och säkerhet i enlighet med definierade mål. Det finns även lagar och förordningar att förhålla sig till.

Styrelsen ska säkerställa att ledningen förstår ramarna för sina befogenheter, och inte på egen hand fattar beslut gällande upphandlingar som kräver att styrelsen involveras.

Vid upphandling som avser att låta annan part hantera leverans av tjänster, bör vikt läggas vid att tjänsteleveransen bidrar till att skapa det värde som efterfrågas och de nyttor som definierats. Även om en tjänst läggs på en extern part, kvarstår ansvaret hos organisationen och därmed styrelsen.

I vissa fall kan styrelsen agera bollplank till ledningen utan att delta i operativa beslut. När en upphandling omfattar betydande belopp och komplexitet bör styrelsen hållas informerad och vara tillgänglig för att behandla frågor som lyfts från ledningen.

Styrelsens eget ställningstagande:

- Har vi, eller avser vi att behålla, en egen IT-drifts-organisation och i så fall med vilken inriktning?
- Hur ser identifieringen ut av vilken typ av information en eller flera leverantörer inte får hantera eller ha åtkomst till?
- Vilka är våra krav på leverantörens tillgänglighet i form av geografi, geopolitik, kontaktpersoner samt andra verksamhetsspecifika förutsättningar?
- Hur tydlig är vår investeringspolicy och instruktion för verkställande ledning, och reglerar denna hur långa kontrakt samt hyres- eller leasingavtal ska hanteras?

Styrelsens frågor till ledningen:

- Hur säkerställer ledningen leverantörers stabilitet?
- På vilket sätt utvärderas partners avseende leverans av funktionalitet, kvalitet och informationssäkerhet?

Styrning av värdesäkring

För att få ut önskat värde av de resurser som verksamhetens IT har tillgång till, bör styrelsen ha en kontinuerlig och strategiskt inriktad dialog med verkställande ledning för att säkerställa att interna processer utvecklas och optimeras. Det önskade värdet bör inte begränsas till enbart ekonomi, utan kan även avse nöjdhet hos kunder och medarbetare. En del i detta är att sätta tydliga och utmanande mål för transformationsprogram. Effekten av transformationsprogram måste följas upp med både kvantitativa och kvalitativa mätvärden, vilka även kan beskriva hur befintliga lösningar ger värde i framtiden. Där det är möjligt kan den egna verksamheten jämföras med andra likvärdiga verksamheter, både sådana som anses bättre än genomsnittet och sådana som anses sämre än genomsnittet.

Riskvillighet och resursoptimering har en direkt påverkan på utfallet. Det kan bli aktuellt att ompröva tidigare beslut, framför allt när det sker större förändringar på marknaden eller i verksamhetens omgivning. Verksamhetens IT påverkas med jämna mellanrum av teknikskiften som kan vara dyrbara om verksamheten hamnar på efterkälken och därmed förlorar strategiska möjligheter. Sådana skiften kan också leda till stor påverkan om beslut har fattats i en teknologisk riktning som inte är framtidssäkrad. Styrelsen kan därför behöva ge ledningen tydliga direktiv att överge beslut som de har investerat sin framtid i.

Styrelsens eget ställningstagande:

- Hur har styrelsen säkrat sin förmåga att agera när ledningen inte tar till sig av ifrågasättande av valda teknikinriktningar?
- På vilket sätt kan styrelsen arbeta för att överbrygga missförstånd i språkbruk när det gäller teknologiska termer?
- Hur har styrelsen säkrat nödvändig kompetens för att göra relevanta bedömningar vid prioritering av olika investeringsalternativ?

Styrelsens frågor till ledningen:

- Hur har ledningen genomfört och dragit lärdom av genomförda transformationsprogram?
- Hur har ekonomistyrmodeller utvecklats i takt med förändringar i verksamhetens IT, och hur säkerställs kvalitet i den ekonomiska rapporteringen?
- På vilket sätt har den strategiska planen och verksamhetsutveckling med IT beaktats?

Om detta dokument

Denna vägledning är resultatet av ett initiativ taget av ISACA Sweden och IIA Sweden. Några av personerna i arbetsgruppen har medverkat i framtagandet av vägledningen på ideell basis, medan andra har haft arbetsgivarens tillåtelse att medverka på arbetstid. Tack för allas bidrag!

ISACA Sweden Chapter är en del av den internationella bransch-organisationen Information Systems Audit and Control Association (ISACA). ISACA har cirka 750 medlemmar i Sverige och över 170 000 globalt som arbetar med verksamhets- och IT-ledare 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 med-lemmar i Sverige och över 235 000 globalt som arbetar med intern-revision, 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.

Vägledning är relaterad till publikationen ”Stöd för revision av verksamhetens IT”, framtagen av ISACA Sweden och IIA Sweden, en publikation som vänder sig till revisorer och IT-revisorer där specifika kontrollområden valts ut.

Deltagare
John Wallhoff – ISACA Sweden
Thomas Verner – ISACA Sweden
Ann-Katrin Harringer – IIA Sweden
Stina Nilsson Kristiansson
– Verkställande Direktör (VD) och Generalsekreterare IIA Sweden
Björn Rosenkvist – IIA Sweden
Peter Westberg – IIA Sweden

Referensdeltagare
Mounir Messaoud – ISACA Sweden
Martin Malm - IIA Sweden

Granskare av dokumentet
Miriam Gyllenros – IIA Sweden
Åsa Berglund – IIA Sweden
Hans Tedesund – IIA Sweden
Eva Fredriksson – IIA Sweden
Peter Käll – ISACA Sweden
Kevin Hong – ISACA Sweden
Lars Stenquist – ISACA Sweden
Kim Nordström – ISACA Sweden
Ulf Holmerin – ISACA Sweden
Jonas Malmvall – ISACA Sweden
Alexander Pantus – ISACA Sweden

Organisationer som har arbetat fram vägledningen
Info om IIA Sweden – www.theiia.se
Info om ISACA Sweden – www.isaca.se

ISACA®
Sweden Chapter

IIA
Sweden