2022

Revision av verksamhetens IT

Stöd för revisorer vid granskning av IT-styrning och IT-system

Version: (2022)

Introduktion

Många verksamheter är idag beroende av en väl fungerande IT-miljö och i takt med att beroendet av IT blir allt mer påtagligt är det nödvändigt att resursslöseri och brister hanteras skyndsamt för att inte äventyra verksamheten. Styrelse och ledning ansvarar för att dessa resurser används kostnadseffektivt och att de bidrar till att verksamheten når uppsatta mål. Brister i IT-kontroller kan ha stor påverkan på en organisations finansiella situation och anseende. I detta sammanhang har revisorer en viktig roll att spela genom att förse styrelsen och ledningen med relevant information om hur väl den interna styrningen och kontrollen över IT-miljön fungerar. Internrevisorn har till uppgift att rapportera utfallet av sin revision till ledning och styrelse.

Syftet med detta stöd är att ge en allmän orientering och stöd till generella IT-relaterade områden. Dokumentet är framtaget av IIA Sweden och ISACA Sweden och är därmed skrivet utifrån internrevisorns och IT-revisorns perspektiv. I dokumentet används därför begreppet ”revisor” i denna betydelse. Dokumentet kan dock med fördel även användas av andra yrkeskategorier som har till uppgift att granska, bedöma eller utvärdera riskhantering, ledning samt den interna styrning och kontrollen inom området.

Som underlag till detta dokument har ett antal områden, som kan vara relevanta att granska, valts ut utifrån arbetsgruppens uppfattning om vanligt förekommande riskområden. För respektive område har några nyckelkontroller valts ut. Nyckelkontrollerna som föreslås i detta dokument utgår från ramverk och råd som har utvecklats av IIA och ISACA på global nivå. Nyckelkontrollerna har formulerats med hänsyn tagen till de förutsättningar som är relevanta för Sverige. Även andra publikationer, vilka har etablerats som de facto-standards och rekommendationer för att hantera IT med god kontroll, har beaktats i detta dokument.

Som nämnts ovan kan brister i IT-kontroller allvarligt påverka t.ex. ekonomisk rapportering, verksamhet och anseende. Det är därför viktigt att säkerställa att revisorn i en granskning kommunicerar faktabaserade och objektiva iakttagelser och identifierar relevanta risker och brister. Det är, i detta sammanhang, av största betydelse att revisorn försäkrar sig om att rätt kompetens finns i teamet. Det vi hoppas förmedla med denna skrift är att beskriva att vissa IT-frågor kan hanteras av en revisor med generell revisionskompetens, medan andra IT-frågor kräver involvering av experter med djupare ämneskunskaper för att navigera i organisationens IT-miljö. Specialister inom IT-revision kan behöva involveras för att adressera områden där specialistkunskaper inom specifika delar är nödvändiga.

Granskningsområden

Strategi och styrning av IT-verksamheten

IT-styrning syftar till att hantera organisatoriska processer på ett sätt som skapar värde till organisationen och att de beslut som fattas om anskaffning och fördelningen av IT-resurser är väl underbyggda och motiverade. En effektiv IT-styrning förutsätter samordning av verksamhetsstrategi, strategiska beslut och IT-strategi för att säkra att verksamhetens IT upprätthåller och förstärker organisationens strategier och mål. I styrningen ingår beaktande av befogenheter och behörigheter, kontroller, redovisningsskyldighet samt roller och fördelning av ansvarsområden mellan organisatoriska enheter. IT-styrningen omfattar även identifiering, värdering och hantering av de IT-relaterade risker som uppkommer i verksamheten. I detta ingår IT-förvaltning och IT-utveckling.

Nyckelkontroller:

- Det ska finnas en tydlig koppling mellan IT-strategi och verksamhetsstrategi
- Riskanalys ska genomföras för att identifiera och därefter hantera de mest väsentliga riskerna genom nyckelkontroller IT-investeringar ska utvärderas och formellt beslutas för att ge värde till organisationen och främja effektiv användning av IT-resurser
- Utfallet av IT-verksamheten ska definieras samt mätas och rapporteras på ett ändamålsenligt sätt
- Ledningen ska vara involverad i IT-styrningen
- Det ska finnas en tydlig ansvarsfördelning och kommunikation mellan verksamheten och IT-avdelningen, samt inom IT-avdelningen.

Standarder och referensmaterial:

- COBIT 2019
- Auditing IT Governance (IIA GTAG)
- IT Essentials for the Internal Auditors (IIA GTAG)
- ISO 38500 Governance of IT for the organization
- SAFe (Scaled Agile Framework)

Styrning av informations-säkerhet

Information har blivit en extremt kritisk tillgång för många organisationer och risken för informationsstöld och utpressningsmjukvara blir allt större. I en allt mer uppkopplad värld använder många organisationer ett ledningssystem för informationssäkerhet (LIS) som ett sätt att strukturera arbetet med att säkerställa att informationstillgångarnas konfidentialitet, integritet och tillgänglighet motsvarar verksamhetens behov. Styrning av informationssäkerhet har även en direkt påverkan på verksamheters dataskyddsarbete enligt dataskyddsförordningen (GDPR).

De kontroller som är tillämpliga avseende styrning av informationssäkerhet innefattar en förteckning över specifika säkerhetsåtgärder i ISO-standarden. Dessa säkerhetsåtgärder är teknikneutrala, vilket innebär att ytterligare vägledning kan behövas för att identifiera vilka förutsättningar som råder för en specifik teknisk komponent. Detta avser även cybersäkerhet, ett område som fokuserar på granskning av skyddsåtgärder avseende externa hot och attacker.

Nyckelkontroller:

- Det ska finnas strukturerat och systematiskt informationssäkerhetsarbete där ledningen verifierar att detta arbete utförs enligt direktiv, ger styrning och tillsätter nödvändiga resurser
- Det ska finnas en informationssäkerhetspolicy eller motsvarande
- Informationsklassificering ska genomföras
- Val av och implementering av säkerhetsåtgärder ska göras utifrån verksamhetens behov
- Informationsspridning och utbildning sker regelbundet.

Standarder och referensmaterial:

- ISO/IEC 27001 Ledningssystem för informationssäkerhet
- ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder
- MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter
- MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
- MSBFS 2020:8 föreskrifter om rapportering av IT-incidenter för statliga myndigheter
- GDPR/dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter)
- SSF 1101 Cybersäkerhet Bas
- NIST Cyber Security Framework
- Center for Internet Security, CIS Controls

Kontinuitets-hantering

Kontinuitetshantering handlar om systematisk planering för att upprätthålla verksamheten på acceptabla nivåer avseende drift och hantering av data, oavsett vilken störning den utsätts för. Detta genomförs med fördel genom att identifiera vilka delar av verksamheten som måste fungera för att organisationen inte ska drabbas av allvarliga konsekvenser vid en störning, vilka kritiska resurser som krävs för att upprätthålla dessa delar av verksamheten samt att planera för hur respektive kritisk resurs ska hanteras om den slås ut.

Planerna bör ange roller och ansvar samt en process för ett aktivt agerande under och efter en incident för att hantera de omedelbara konsekvenserna av ett avbrott i en eller flera nödvändiga resurser.

Nyckelkontroller:

- Verksamhetskritiska processer och områden ska fastställas
- Nödvändiga resurser (individer, lokaler, IT-komponenter) ska identifieras och analyseras
- För kritiska verksamhetsområden/processer ska acceptabla servicenivåer definieras och konsekvenser av eventuella störningar i dessa verksamhetsområden /processer identifieras
- Kontinuitetsplaner för prioriterade verksamhetsområden /processer ska upprättas
- Dokumenterade rutiner ska upprättas för att återuppta och återställa verksamheten efter ett avbrott
- Regelbunden övning och testning ska genomföras för att säkerställa att rutiner och förmågor är förenliga med organisationens kontinuitetsmål.

Standarder och referensmaterial:

- Business Continuity Management (IIA GTAG)
- ISO 22301 Ledningssystem för kontinuitet
- MSB: En lathund för arbete med kontinuitetshantering

Hantering av utlagd verksamhet och tjänster inom IT

Organisationer använder sig ofta av externa leverantörer av IT-tjänster, exempelvis molntjänster. 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. Vikt bör även läggas vid att tjänste-leveransen bidrar till att verksamheten kan uppnå sina mål och skapa det värde som efterfrågas och de nyttor som definierats. Även om en tjänst läggs på en extern part, kvarstår ansvaret hos organisationen.

Nyckelkontroller:

- Inköp och upphandling av tjänster ska omfattas av en objektiv urvalsprocess där verksamhetens behov beaktas
- Grundläggande säkerhetskrav som minst motsvarar verksamhetens egen säkerhetsnivå ska regleras i avtal och uppfyllas
- Leverantörer ska endast ha tillgång till den information som är nödvändig för att kunna leverera avtalade tjänster
- En uppföljning av levererade IT-tjänster ska göras regel-bundet där omfattningen bestäms i en riskanalys.

Standarder och referensmaterial:

- COBIT 2019
- Information Technology Outsourcing (IIA GTAG)
- ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder
- MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8 och 2020:6)
- Cloud Security Alliance - CSA Security Guidance.

Hantering av IT-utveckling

De flesta organisationer har behov av IT-stöd för genomförande av sin verksamhet. Systemstöd kan tillhandahållas antingen i form av färdig programvara eller genom utveckling. Vilket alternativ som bedöms vara mest ändamålsenligt för verksamheten beror på flera olika faktorer, till exempel befintlig systemmiljö och hur standardiserat verksamhetens behov är.

IT-utveckling avser dels nyutveckling, dels vidareutveckling av befintliga system. Detta ingår vanligen i den löpande förvaltningsstyrningen. Utveckling av IT-miljö och system-lösningar bör ske på ett strukturerat och enhetligt sätt för att säkerställa tillräcklig kvalitet och säkerhet. När det gäller förvaltningsstyrningen krävs ofta ett visst löpande arbete för att systemstödet ska fortsätta leverera värde. På senare tid har många organisationer lämnat traditionella modeller för styrning av utveckling och förvaltning och övergått till agila arbetssätt för att snabbare kunna leverera värde.

Nyckelkontroller:

- Det ska finnas en tydlig definition av målet med utvecklingen eller önskad effekt från den utveckling som föreslås
- Användare- eller användarrepresentanter ska involveras i framtagandet av funktionella ändringar som påverkar slutanvändarna
- Roller och ansvar för utvecklingsprocessen ska vara definierade
- Icke-funktionella krav och säkerhetsrisker ska utvärderas i utvecklingsprocessen
- Testning ska göras utifrån de behov som är relevanta för utvecklingsarbetet
- Genomförd utveckling och testning ska vara spårbar
- Uppföljning av progress, nedlagt tid och budget ska ske löpande
- Vid större förändringar ska levererade effekter efter införandet följas upp.

Standarder och referensmaterial:

- COBIT 2019
- Auditing IT Projects (IIA GTAG)
- SAFe Scaled Agile Framework

Hantering av IT-drift

Driften av IT inom en organisation innehåller planering, samordning, övervakning och uppföljning av leveransen av IT-tjänster inklusive genomförande av fördefinierade drifts-förfaranden samt nödvändiga övervakningsaktiviteter.

För att snabbt kunna agera på störningar och dataintrång övervakas aktiviteter i nätverk och system. Detta kan göras i förebyggande syfte för att identifiera svagheter i arkitektur, konfiguration och version av programvara. För att övervaka den dagliga driften sparas spår av inloggning och användande på ett sådant sätt att det är möjligt att upptäcka oönskat nyttjande, vilket innebär att denna information finns sparad i en eller flera loggar. En del organisationer tillämpar ”DevOps”, en uppsättning arbetsmetoder som främjar samarbete eller integration mellan IT-utveckling och IT-drift.

Nyckelkontroller:

- Operativa driftrutiner för levererade IT-tjänster, inklusive hantering av backuper och schemalagda systemjobb ska utvecklas och underhållas
- Ett aktuellt register över alla IT-tillgångar och deras beroenden samt deras kontinuerliga uppdatering ska finnas
- En process för konfigurationshantering av tjänster, tillgångar och infrastruktur samt relationerna mellan dem ska finnas
- Förebyggande och upptäckande kontroller för hantering av säkerhetsuppdateringar (patchning) för att skydda informationssystem och teknik från skadlig kod ska vara etablerade
- Teknisk analys av sårbarheter i utrustning och system ska göras regelbundet
- System och nätverksloggar ska sparas, med begränsad åtkomst, och vara tillgänglig för uppföljning
- Kontinuerlig genomgång av loggar ska göras och det ska finnas en funktion för övervakning av larm i driftsmiljön
- Det ska finna rutiner för att hantera programvarulicenser så att antalet installerade licenser överensstämmer med verksamhetens krav och antalet ägda licenser.

Standarder och referensmaterial:

- COBIT 2019
- Auditing Business applications (IIA GTAG)
- ISO/IEC 20000-1 Ledningssystem för tjänster
- Center for Internet Security, CIS Controls
- Center for Internet Security, CIS Benchmarks

Åtkomst och behörigheter

Åtkomstbegränsningar till och i system och nätverk behöver finnas på plats för att rätt användare har tillgång till rätt information utifrån organisationens klassificering av dess informationstillgångar. Dessa begränsningar är nödvändiga för att IT-systemen inte skall kunna missbrukas av obehöriga. Styrning av behörigheter bör utformas utifrån användarnas roller och arbetsuppgifter, samt följas upp med ändamålsenlig regelbundenhet. Begränsning och kontroll av administratörsrättigheter är av särskild vikt, då dessa användare innehar mer omfattande behörigheter än andra.

Nyckelkontroller:

- Användares identitet ska verifieras för att säkerställa att rätt person har tillgång till information och funktioner
- Användare ska autentiseras för att förhindra obehörig åtkomst till samt användning av information och funktioner
- Rolluppsättningen i system ska säkerställa åtskillnad /separation av ansvars-/arbetsuppgifter
- Användare ska enbart ha tillgång till den information de är i behov av för att genomföra sina arbetsuppgifter
- Tilldelning och ändring av behörigheter ska godkänns av behörig person, exempelvis av informationsägare och/eller systemägare
- Regelbunden granskning/genomgång av befintliga behörigheter ska utföras och inaktuella användare /behörigheter ska tas bort
- Konton med administratörsbehörigheter bör använda tvåfaktorsautentisering.

Standarder och referensmaterial:

- COBIT 2019
- Identity and Access Management (IIA GTAG).
- ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder
- NIST 800-53

Hantering av förändringar i IT-miljö och IT-system

Moderna IT-miljöer är ofta komplexa och består av många komponenter som utvecklas, förvaltas och driftas internt eller av extern part. Att ha kontroll på allt som förändras i en sådan miljö är en grundförutsättning för tillförlitlig drift och leverans av IT-tjänster till interna och externa kunder. Olika delar av IT-miljön kan ha olika processer för hantering av förändringar men samma typ av god praxis bör tillämpas oavsett typ av förändring. Hur processen kan se ut varierar, likaså graden av automatisering. I ett modernt CI/CD-flöde (continuous integration/continuous delivery) sker många av kontrollmomenten i de verktygen som används i flödet t.ex. automatiska tester samt kontroll mot kända säkerhetsbrister.

Nyckelkontroller:

- Det ska finnas en process för införande av IT-förändringar i produktionsmiljön
- Införande av ändringar ska prioriteras, tidsättas och godkännas utifrån verksamhetens behov innan de produktionssätts
- Ändringar ska analyseras för att identifiera beroenden /påverkan på andra delar i miljön
- Tillräcklig spårbarhet från genomförda driftsättningar ska finnas för att kunna underlätta hantering av eventuella uppkomna incidenter, samt att kunna ta fram lämpliga mätetal
- Produktionssättning ska föregås av ändamålsenlig testning och annan nödvändig kvalitetssäkring
- Särskilda rutiner ska finnas för att hantera akuta ändringar.

Standarder och referensmaterial:

- COBIT 2019
- ISACA Change Management Audit Program.
- IT Change Management:
  Critical for Organizational Success (IIA GTAG)
- ISO 27002 Riktlinjer för informationssäkerhetsåtgärder

Hantering av IT-tjänster och IT-incidenter

En effektiv försörjning av IT-tjänster och IT-utrustning sker genom en rutin för beställningar, som möjliggör för medarbetare att snabbt få tillgång till rätt verktyg eller system för att kunna utföra sitt arbete. Det bör även finnas rutiner för att åtgärda fel eller störningar, som innebär att arbete inte kan utföras eller tar längre tid än nödvändigt. När fel eller störningar återkommer finns det betydande vinster med att gå på djupet i att identifiera de bakomliggande orsakerna. Det är också nödvändigt att bli uppmärksammad på de incidenter som innebär en säkerhetsrisk, exempelvis stöld eller läckage av känslig information samt information som berör den personliga integriteten. Vissa incidenter kan behöva rapporteras till extern part.

Nyckelkontroller:

- Beställningar av IT-tjänster och -utrustning till nya användare och ändringar för befintliga användare ska hanteras så att det stödjer verksamhetens behov
- Det ska finnas ett systematiskt tillvägagångssätt för rapportering, och registrering och hantering av fel och incidenter vid utnyttjande av IT-system, samt vid säkerhetsbrister
- Återkommande fel och incidenter i IT-system ska analyseras för att identifiera och i möjligaste mån eliminera underliggande orsaker till dessa fel.

Standarder och referensmaterial:

- COBIT 2019
- ISO/IEC 20000-1 Ledningssystem för tjänster
- ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder
- ITIL 4

Fysisk säkerhet

Verksamhetens utrustning och lokaler behöver vara skyddade mot intrång och yttre påverkan som kan leda till stöld av kritiska informationstillgångar, eller andra störningar i verksamheten. Det är också av stor vikt att säkerställa att verksamhetens IT-system i möjligaste mån inte påverkas negativt av externa faktorer såsom oväder, jordskred eller liknande händelser.

Nyckelkontroller

- Det ska finnas ett skalskydd som innebär att obehöriga inte kan komma in i kontorslokaler eller datahallar utan tillstånd
- Regler för hantering av tillhandahållen IT-utrustning ska formuleras, dokumenteras och kommuniceras.
- IT-utrustning som användare kan ta med sig utanför verksamhetens lokaler ska hanteras enligt uppsatta regler
- IT-utrustning ska vara skyddad mot påverkan av ström-avbrott, väderfenomen och andra händelser som ligger utom verksamhetens kontroll
- Åtkomst till kritisk IT-utrustning ska vara begränsad och hanteras enligt fastställd behörighetsrutin.

Standarder och referensmaterial

- COBIT 2019
- ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder

Terminologi

Agile
Agile (agilt) används inom IT-området som ett samlingsnamn för olika metoder inom systemutveckling, där krav på funktionalitet förändras allt eftersom arbetet fortskrider.

Applikation
Datorprogram som används för arbete, informationsinhämtning, underhållning eller spel, dvs. program som motiverar att man använder datorn. Applikationer ska skiljas från program som får datorn att fungera. Det kan avse systemprogram som t.ex. operativsystem, drivrutiner och kommunikationsprogram som får datorn att fungera, eller verktygsprogram som behövs för att själva datorn, dess tillbehör och nätet ska fungerar.

Applikationskontroll
Kontroller som finns i enskilda applikationer/system som säkerställer fullständigheten och noggrannheten i manuell registrering av data samt bearbetning av data genom programkod.

Arkitektur
Ett sätt att organisera resurser och komponenter i ett datorsystem. Det kan avse IT-infrastruktur där komponenterna består av olika hårdvara och gränssnitt. IT-arkitektur kan också avse uppbyggnaden av en dator eller ett informationssystem, där komponenterna består av mjukvara och gränssnitten av standardiserade dataspecifikationer eller kommunikationsprotokoll.

COBIT
Ett ramverk för styrning och ledning av en verksamhets information och teknologi. En samling av generellt accepterade och applicerbara standarder för främst informationsteknologi.

DevOps
En uppsättning metoder som kombinerar mjukvaruutveckling och IT-drift. Det syftar till att förkorta systemutvecklingens livscykel och tillhandahålla kontinuerlig leverans med hög mjukvarukvalitet. DevOps kompletterar agil mjukvaruutveckling och flera DevOps-aspekter kommer från Agile-metodiken.

Förvaltningsstyrning
Görs i syfte att kontinuerligt stödja, vidmakthålla, vidareutveckla och tillgängliggöra IT-produkter. Förvaltningen kan organiseras utifrån objekt, funktion, system och applikation.

GDPR
En europeisk förordning som reglerar behandlingen av personuppgifter och det fria flödet av sådana uppgifter inom Europeiska unionen.

Generella IT-kontroller
Kontroller som omfattar säkerställandet av korrekt användar- och behörighetshantering, utveckling, implementering och underhåll av alla applikationer i en IT-miljö, samt kontroller avseende IT-drift.

Informationsklassificering
En process inom informationssäkerhetsarbetet för att klassificera hur information ska hanteras och behandlas. För att kunna ge rätt skyddsnivå för information måste företag/organisationer veta vilken information som är skyddsvärd och varför den är det.

IFAC (International Federation of Accountants)
Global organisation för auktoriserade och godkända revisorer som stödjer utvecklingen, antagandet och implementeringen av internationella standarder av hög kvalitet.

ISO (International Organization for Standardization)
Internationell standardiseringsorganisation som arbetar med industriell och kommersiell standardisering. ISO har gett ut ett stort antal standarder, t.ex. avseende informationssäkerhet.

ITIL (Information Technology Infrastructure Library)
En samling principer för hantering av IT-tjänster som innehåller detaljerade beskrivningar av hur olika IT-relaterade uppgifter kan utföras.

Molntjänst
IT-tjänst/-er som tillhandahålls över internet. Det kan till exempel handla om tillämpningsprogram, serverprogram och lagring av data.

NIST (National institute of standards and technology)
Amerikansk federal myndighet som utvecklar och fastställer standarder, bland annat för IT. Ramverket för IT-säkerhet kallas för NIST-CSF – cyber security framework.

SAFe (Scaled Agile Framework)
En verktygslåda för att tillämpa agila metoder på ett helt företag eller en hel organisation under utveckling

Tvåfaktorsautentisering
En metod för att verifiera (autentisera) en användare som begär åtkomst till ett system. Användaren måste verifiera sin identitet genom en kombination av två olika komponenter, exempelvis ett lösenord och en kod som genereras via mobiltelefon.

Om detta dokument

Detta dokument är resultatet av ett initiativ taget av ISACA Sweden och IIA Sweden. Vissa personer i arbetsgruppen har medverkat i framtagandet av dokumentet på ideell basis, medan andra har haft arbetsgivarens tillåtelse att medverka på arbetstid. Tack för allas bidrag!

Deltagare i arbetsgruppen

Jens Ryning
– ISACA Sweden
John Wallhoff
– ISACA Sweden
Magnus Thyllman
– IIA Sweden och ISACA Sweden
Mounir Messaoud
– ISACA Sweden
Peter Westberg
– IIA Sweden och ISACA Sweden
Stina Nilsson Kristiansson
– Vd och Generalsekreterare IIA Sweden
Taif Al Mobarek
– ISACA Sweden

Granskare av dokumentet
Förening auktoriserade revisorer (FAR)
Professionsutvecklingskommittén inom IIA Sweden

Organisationer som har arbetat fram dokumentet
Info om IIA Sweden - www.theiia.se
Info om ISACA Sweden - www.isaca.se

ISACA®
Sweden Chapter

IIA
Sweden