



PANIC

It-sikkerhed

Artikel trykt i It-sikkerhed.
Gengivelse af denne artikel
eller dele heraf er ikke tilladt
ifølge dansk lov om ophavsret.

Børsen Ledelseshåndbøger er
Danmarks største og stærkeste
videns- og udviklingsklub. Uanset
hvilket område eller emne du
beskæftiger dig med, får du her
et komplet opslagsværk på print,
cd-rom og internet, der giver
dig overblik og indsigt.

Ledelseshåndbogen er et praktisk
og overskueligt værktøj til dig,
der vil være 100% opdateret
inden for et bestemt område
– selvom du har en travl hverdag.

© Børsen Forum A/S, 2008

Compliance, kvalitetssikring og optimering

af direktør Frederik Helweg-Larsen, fhl@policyenforcer.dk,
CISM, Policy Enforcer ApS

Compliance bliver tit opfattet som en tilstand for eliten, der har næsten ubegrænsede ressourcer og besidder et fantastisk overblik over hele deres organisation - ligesom ledelsen naturligvis bakker hundrede procent op. Sådan er virkeligheden sjældent, men det er ikke så svært at komme i gang.

Det at være *compliant* opfattes af mange som næsten uopnåeligt, men er basalt set et spørgsmål om, hvad det er, man har behov for at være compliant med. Det kan være lovgivning, sikkerhedsstandarder, kvalitetsstandarder, revisionsstandarder eller virksomhedens politikker i bred forstand. Den første øvelse ligger altså i at kortlægge de love, regler og standarder som man skal følge.

Dette er ikke nødvendigvis nogen lang liste, men den er utrolig vigtig at være opmærksom på, og er det rigtige sted at starte opfølgningen. Selvom der allerede er godt styr på disse standarder og regler, så er det vigtigt at kunne dokumentere opfølgning og efterlevelse over for myndigheder og revision.

Når kravene fra omverdenen er håndteret, skal ambitionsniveauet sættes for de øvrige områder, og her bør man fokusere på de regler og processer, der rent faktisk bidrager til virksomhedens bundlinje.

1. Indledning

Hvad forstår vi ved compliance?

Compliance er ikke en entydig tilstand. Oversat til dansk betyder det "efterlevelse af krav", uden at der refereres til nogle specifikke krav. Disse krav kan være opstillet af lovgivning, regulative krav, omverdenen eller virksomheden selv. Ofte er kravene branchespecifikke eller afhængige af, i hvilke lande man driver forretning.

Inden vi kan tale om at være *compliant*, må vi altså definere, hvilke regler eller krav vi har behov for at dokumentere, at vi efterlever. Er dette ikke klart, eller er man i tvivl, vil en af de virksomheder, der udbyder sikkerhedsrådgivning, kunne hjælpe.

I denne artikel vil jeg behandle emnet compliance med informationssikkerhed som udgangspunkt, men principperne er de samme, uanset hvilken form for politik man ønsker at implementere og følge op på.

Kan det betale sig?

Det vil være oplagt for virksomhedsledelsen at starte med at vurdere, om det overhovedet kan betale sig at kunne dokumentere efterlevelsen af en standard eller en række af krav. For at kunne vurdere dette skal man både kigge på, hvad man opnår, og hvad man undgår.

Det kan være meget vanskeligt at påvise *Return-Of-Investment* (ROI) på en sikkerhedsløsning, da sikkerhed primært handler om at undgå uønskede hændelser. Da vi ikke bagefter kan påvise, hvad det var, vi undgik, vil gevinsten ofte være et estimat eller en vurdering.

Kigger man derimod på, hvad organisationen opnår ved at have klart beskrevne politikker og have en konsekvent opfølgning på de områder, der er kritiske for at drive forretning, er fordelene mere håndgribelige. Lad mig her nævne nogle eksempler på oplevet udbytte baseret på erfaringer.

Hvad man opnår

Det meste af det, man opnår ved at have korrekt udformet, formuleret og implementeret politik for informationssikkerhed, er fordele, der hurtigt vil vise sig, og er meget håndgribelige:

- Fælles referenceramme og afstemning af forventninger
- Klar fordeling af ansvar og opgaver
- Optimering af eksisterende arbejdsprocesser
- Ensartet kvalitet
- Smidighed ved vækst og tilgang af nye medarbejdere
- Grundlag for prioritering af ressourceforbrug

- Grundlæggende risikovurdering
- Basis for beredskabsplanlægning
- Besparelser i forhold til revision.

Erfaringsmæssigt opleves den indbyrdes kommunikation, og følgende ensretning af målsætninger, som den mest markante fordel ved opstarten af et *compliance*-projekt. Arbejder man med informationssikkerhed, er det noget, der vedrører alle funktioner i organisationen – men ofte er den enkelte afdelingsleder ikke bekendt med sit ansvarsområde, de konkrete mål og den vigtige rolle han eller hun udgør i det samlede billede.

For enhver type af ledelse er det afgørende, at alle kender målene og trækker i samme retning for at opnå de ønskede resultater. Denne første erkendelse gør et indtryk på de fleste men forpligter også, da beslutningerne bagefter skal implementeres.

Hvad man undgår

Det er betydeligt sværere at dokumentere, hvilke situationer der er undgået, da de i sagens natur ikke har fundet sted. Derimod er det tydeligt for de fleste, at klart definerede arbejdsprocesser, der følges op med faste intervaller, minimerer risikoen for fejl og dermed uønskede hændelser.

Dette er nogle eksempler på, hvad man kan undgå ved at have en politik for informationssikkerhed, der efterleves og følges op:

- Uheldige episoder med medarbejdere der ikke kender reglerne
- Uklarhed om placering af ansvar
- Uklarhed om mål, regler og forventninger
- Demotiverende politikker der ikke efterleves
- Udefrakommende uønskede hændelser (?).

Man kan naturligvis ikke gardere sig imod fejl eller medarbejders overlagte brud på reglerne, men man kan demonstrere ledelsens klare holdninger og indsatser for at minimere, at den slags forekommer. Det er god og ansvarlig virksomhedsledelse.

Kvalitetssikring kan være en anden tilgang

Det kan være svært at retfærdiggøre et projekt, der kun har til formål at sikre efterlevelsen af nogle krav eller standarder, som virksomheden ikke har noget særligt forhold til. Det bliver let en ubejljet nødvendighed, som ikke får den store opbakning fra organisationen. Det skyldes primært, at den enkelte medarbejder ikke kan se relevansen i hverdagen.

Derfor vil det ofte være bedre at tage udgangspunkt i den forretningsmæssige værdi i at have en ensartet kvalitet i de vigtigste arbejdsprocesser og sikre, at der er fokus på, at de mest kritiske processer bliver dokumenteret og sikret.

Ved at tage fat i virksomhedens kerneforretning bliver arbejdet betydelig mere relevant, og det er tydeligt for de fleste, at kvalitet og optimering er noget, der styrker markedspositionen og forbedrer konkurrenceevnen. Det kan med andre ord betale sig.

Samtidig skal man selvfølgelig have alle relevante krav med, men det er vigtigt, at de ikke står alene. Sørg for, at der er fokus på optimering af jeres eksisterende arbejdsopgaver for at få maksimal opbakning.

2. Inden I går i gang

Valg af standarder eller rammeværktøjer

Det er et meget stort arbejde at starte med et blankt stykke papir og begynde med at definere politikker og procedurer på "fri hånd". Derfor kan det anbefales at anvende en eller flere standarder inden for det område, man vil arbejde med. Disse standarder er som oftest gode "checklister", som man kan arbejde ud fra, men de giver ofte anledning til at stille flere spørgsmål, end de giver svar.

Der er altså stadig en opgave i at fortolke standarderne og tage stilling til, hvorledes de konkret skal implementeres i organisationen. Her er nogle af de standarder eller rammeværktøjer, I kan støde på, når I skal arbejde med informationsikkerhed. Det er ikke en komplet liste men blot nogle almindeligt forekomne eksempler.

Standard	Beskrivelse
DS 484:2005	Dansk Standard for it-sikkerhed. Behandler informationssikkerhed meget bredt og dækker meget mere end den tekniske it. Kan ikke implementeres af en it-afdeling alene og kræver hele organisationens deltagelse. Stærkt inspireret af ISO-standard. Staten er underlagt et krav om at følge denne standard.
ISO27001/ISO27002	Den internationale parallel til DS484, der dækker de samme områder med næsten fuldt overlap. Et godt valg for internationale virksomheder, der ønsker en enkel måde at kommunikere, hvilke overvejelser de har været igennem.
COBIT	En omfattende standard for <i>Corporate IT Governance</i> , der dækker bredt, men er betydelig mere detaljeret end DS og ISO. Denne standard er til fri download på: www.isaca.org
ITIL	<i>Information Technology Infrastructure Library</i> (ITIL) er en justerbar struktur, som beskriver de bedste fremgangsmåder for at levere kvalitetsservice og beskæftiger sig meget med de processer, der fører til de ønskede resultater.
Sarbanes Oxley	Amerikansk standard, der blev indført efter ENRON-skandalen med det formål at stramme reglerne for god selskabsledelse. Alle virksomheder, der har aktiviteter i USA eller er på den amerikanske børs, er underlagt SOX.
EuroSox	Et kælenavn for EU's 4., 7. og 8. direktiv. Fokuserer på regler for revision og regnskabsaflæggelse. Det meste er allerede inkluderet i den danske lovgivning.
Basel II	En international standard for de regulativer, der vedrører finansielle institutioner.
FDA	En international (amerikansk) standard for de regulativer, der vedrører medicinalindustrien.

Tabel 1.

Brug af software

Hvis I ønsker at komme hurtigere i gang og bruge tiden på beslutninger frem for formuleringer, kan det være relevant at se på nogle af de standardværktøjer, der er på markedet. Der er flere leverandører af softwareapplikationer til *compliance management*, der leverer færdige fortolkninger og best practices af de mest udbredte standarder.

Software alene løser ikke opgaven, men det er en effektiv måde at styre projektet og sikre den fortsatte fremdrift, når dagligdagen presser sig på, og fokus ændrer sig. Det er også en måde at sikre informationernes tilgængelighed for alle involverede, så den projektansvarlige ikke kommer til at udgøre en sikkerhedsrisiko i kraft af sin position.



Figur 1. Skærbillede fra Policy Enforcer® Compliance Management Software. Kilde: www.policyenforcer.dk

Når I skal vurdere, hvilken software der skal anvendes, er det værd at overveje følgende:

- Er det baseret på kendte og anerkendte teknologier?
- Er der mulighed for regelmæssig automatiseret opfølgning?
- Kan man arbejde med forskellige niveauer for *compliance* i organisationen?
- Sikrer det, at ledelsen får en rapportering, der er forståelig og overskuelig?
- Kan platformen anvendes til opfølgning på flere standarder inden for forskellige områder?
- Tal med kundereferencer og brug deres erfaringer.

Der er mange gode erfaringer med at synliggøre beslutninger, ansvar og opfølgninger i software, da det så bliver organisationens projekt og ikke et enkelt individs opgave. Der findes netværksgrupper hos blandt andre Dansk Industri, Dansk IT, ISACA og ISSA, og det kan være nyttigt at mødes med andre og udveksle erfaringer.

3. Opstart af projektet

Tag udgangspunkt i, hvor jeres virksomhed er lige nu

Jeres nuværende standpunkt er et rigtig godt sted at starte. I ved jo hvor I er, og enhver forbedring af den nuværende tilstand vil være til det bedre. I skal derfor sørge for, at jeres sikkerhedspolitik afspejler virkeligheden og ikke bliver et skønmaleri af, hvordan det burde være.

Tænk på, at de medarbejdere, der forventes at følge politikker og retningslinjer, skal have en fornemmelse af, at de er rimelige og realistiske. Ellers vil man blive mødt af modstand fra første færd.

Inden I hæver "overliggeren", skal I være sikre på, at det er noget I kan gennemføre inden for en overskuelig fremtid, da det ellers vil virke demotiverende og få den direkte modsatte effekt.

Fokuser på det vigtige

Politikker er ikke så svære at lave, for formuleringerne er tit bløde og åbne for fortolkninger. Men det er, når vi skal til at definere procedurer for, hvordan vi implementerer disse politikker, at det bliver svært. For nu begynder vi at forpligte os.

Foretag derfor en simpel og pragmatisk risikovurdering. Hvad er vigtigt for vores kerneforretning, og hvad er knap så vigtigt? Hvad kan ramme vores drift (kortsigtet), og hvad kan ramme os på vores image (langsigtet)? I vil sikkert opleve, at der allerede følges op på flere vigtige processer: Aflåsning af bygning, tilslutning af alarm, backup og test af reetablering. Vurder, om der er flere områder, der er vigtige og enkle at implementere og følge op på.

1. I bør have en politik, der dækker bredt. Det er fornuftigt at have taget stilling.
2. Vurder, hvad der er vigtigt ud fra sandsynlighed og konsekvens.
3. Tag udgangspunkt i, hvor I er, og hvad der er realistisk at gennemføre.
4. Prøv at få funktionslederne til at deltage i beslutningerne. Det kommer godt igen.
5. Sæt ikke noget i gang, som I ikke kan gennemføre på kort sigt.
6. Start altid med en succes. Det motiverer og giver fremdrift.

Start med en succes – det motiverer alle

Politikker, procedurer og kontroller er næppe noget, der vækker glæde og entusiasme blandt kollegaerne. Der er en

stor opgave i at fange interessen hos dem, der skal involveres, og det gøres bedst ved at tage fat i den enkeltes hverdag. Hvis der allerede er processer, der følges dagligt, er det vigtigt at få dem dokumenteret, og få foretaget en opfølgning med det samme. Så er den funktion måske allerede *compliant* med de procedurer, der er besluttet.

Det er bedre at starte med, at dokumentere dét, I er gode til, end at sætte kontroller op på nye områder. Vis alle i organisationen, hvor gode de er på væsentlige områder, og hjælp dem med at optimere og dokumentere deres processer. Så er det langt nemmere at komme tilbage med nye tiltag og forslag til forbedringer.

Lav en plan og vær enige om ambitionsniveauet

Det vil være vigtigt for jer at have en plan for det fremtidige arbejde, der dels sætter de mål, som I er blevet enige om, men også synliggør involveringen fra resten af organisationen. Det er næsten umuligt at drive fremad som enkelt mand/kvinde uden bred opbakning – og bestemt ikke opmuntrende.

Sæt nogle milepæle, der er opnåelige, og dokumenter hver enkelt succes, så *compliance* får et godt ry i jeres virksomhed, som noget der understøtter og måske endda fremmer forretningen.

Hold fremdriften – det er let at gå i stå

Alle projekter er spændende, når de påbegyndes, og deltagerne er fulde af optimisme og interesse. Men som tiden går, vil der være andre opgaver og projekter, der presser sig på og tager opmærksomheden. Det kan betyde en gradvis nedprioritering af *compliance* i jeres organisation, da de daglige opgaver kan være svære at konkurrere med.

Det er derfor vigtigt hele tiden at kommunikere værdien af, hvad hvert eneste tiltag giver for de involverede. Det kan være bedre at kommunikere *kvalitetssikring* frem for *compliance*, da det er lettere at forholde sig til som noget værdiskabende. Men overvej altid, hvilken konkret værdi organisationen får af en procedure.

4. Vigtige overvejelser

Vi kender det fra hverdagen, når vi fx færdes i trafikken. Hvis der ikke er nogle konsekvenser ved at overtræde de vedtagne regler, vil der helt sikkert være en del af dem, der ikke bliver efterlevet. Der kan være de kontante konsekvenser ved at blive kørt ned, fordi man ikke stopper for rødt, og

Konsekvenser ved ikke at følge reglerne

vi følger gerne de regler, der er til for at beskytte os selv. I andre situationer har vi måske brug for "hjælp" til at følge reglerne.

På samme måde er det i en virksomhed. De basale leveregler, der er en del af jeres kultur, bliver helt sikkert efterlevet i hverdagen. Men en del af ledelse består i at sikre, at den kultur virksomheden har, også er den rigtige, og at den udvikler sig i den retning, I ønsker. Det kræver af og til adfærd ændringer fra medarbejderne, og det, ved vi, kan være svært.

Derfor er det vigtigt, at vi ikke laver politikker eller regler, som vi ikke har tænkt os at følge op på eller tage alvorligt. Hvis man skal bevare ledelsens troværdighed, må man demonstrere en vilje til at gennemføre de beslutninger, der træffes – med en fast hånd.

Gør derfor op med jer selv, om en given politik kan gennemføres inden for en overskuelig fremtid, hvor lang tid der skal gives til indkøring, og hvad konsekvensen er ved at overtræde denne politik, efter indkøringsperioden er overstået. Husk, at det er bedre med små troværdige fremskridt, end tigerspring der mislykkes.

Niveauet er ikke nødvendigvis det samme i hele organisationen

Hvis jeres organisation er fordelt på flere lokationer, enten nationalt eller internationalt, er der stor sandsynlighed for, at jeres politikker og krav til *compliance* ikke er de samme alle steder. Hvis vi måler alle efter samme fællesnævner, vil politikken virke demotiverende på dem, der aldrig har mulighed for at imødekomme kravene. Det kan fx være bygningens fysiske forhold, der ikke tillader kontrol af de besøgende.

Hvis man opererer i forskellige lande, vil den lokale lovgivning også betyde, at et fælles regelsæt ikke altid er tilstrækkeligt. Så er det sjældent godt nok med en "*one-size-fits-all*" politik.

Giv derfor forskellige dele af organisationen mulighed for at "spille med handicap", så de har samme muligheder for at være *compliant*, blot ud fra nogle andre målsætninger. Der kan også være forhold, der betyder, at et landekontor har særligt skærpede krav i forhold til resten af organisationen.

Denne måde at lave differentieret *compliance* på giver en meget præcis styring af indsatsområderne i en organisation, der ikke er så homogen, som man kunne ønske sig. Det stiller også store krav til viden om de lokale forhold, så det vil

Lad ledelsen følge med i rapporterne

være nødvendigt med lokale tovholdere. En sådan opgave vil sandsynligvis kræve støtte fra et softwaresystem, da informationsmængden ellers hurtigt vil blive uoverskuelig.

Hvis ledelsen ikke deltager aktivt i arbejdet, er det vigtigt at sørge for som minimum, at de er informerede. Giv dem nogle simple og overskuelige rapporter, som de kan spørge ind til, og lad alle beslutninger, indsatser og resultater være synlige. Det kan være med til at øge interessen fra ledelsens side.

Man vil også opleve, at kommunikationen bliver lettere, når alle har samme referenceramme, og både mål, indsatser og resultater er synlige. Handlinger vil udspringe af de overordnede mål og politikker frem for af isolerede problemløsninger.

Modenhed kommer ikke af sig selv

"Jamen det er vi ikke klar til.." – kunne du måske mene. Men hvordan bliver man det? Kun ved at komme i gang og begynde at dokumentere sin nuværende situation og de nærmeste målsætninger vil modenheden blive udviklet. Man opnår ikke noget ved at vente på bedre tider, da der altid vil være udfordringer, som gør det svært at sætte kvaliteten i system.

Det er lidt som at rydde op i bunkerne. Hvis vi udskyder det, bliver de blot større og opgaven sværere. Hvis tiden er knap (hvad den sikkert er), bryd i stedet opgaven op i flere mindre, så den bliver overkommelig. Fokuser på de forbedringer i kvaliteten der opnås, og ikke så meget på den totale opgave.

Der eksisterer flere modeller for vurdering af modenhed og god selskabsledelse, men variationerne er ikke så store. Derfor ses den modenhedsvurdering, der anvendes i COBIT. Hvor ligger I?

Niveau	Beskrivelse af indsatser
0	<p>Nonexistent</p> <ul style="list-style-type: none"> • There is no senior management oversight of it-related activities to ensure that the enterprise's it-goals add value to the organization and to ensure that it-related risks are appropriately managed.
1	<p>Initial/Ad Hoc</p> <ul style="list-style-type: none"> • There is a realization that more formalized oversight of it is required and it needs to be a shared management responsibility requiring the support of top management. • Regular governance practices such as review meetings, creation of performance reports, and investigation into problems take place, but rely mostly on the initiative of the it-management team, with voluntary or co-opted participation by key business stakeholders, depending on current it-projects and priorities. Problems identified are tackled on a project basis with teams formed as necessary to undertake improvements.
2	<p>Repeatable but Intuitive</p> <ul style="list-style-type: none"> • The concept of it-governance does not exist formally and oversight is based mostly on management's consideration of it-related issues on a case-by-case basis. The governance of it depends on the initiative and experience of the it-management team, with limited input from the rest of the organization. • Upper management is involved only when there are major problems or successes. The measurement of it-performance is typically limited to technical measures and only within the it-function.
3	<p>Defined Process</p> <ul style="list-style-type: none"> • An organizational and process framework has been defined for oversight and management of it-activities and is being introduced to the organization as the basis for it-governance. • Specific procedures for management covering key governance activities have been developed. These include regular target-setting, reviews of performance, assessments of capability against planned needs, and project planning and funding for any necessary it-improvements. • Previous informal but successful practices have been institutionalized and the techniques followed are relatively simple and unsophisticated.

4	<p>Managed and Measurable</p> <ul style="list-style-type: none"> • Target-setting has developed to a fairly sophisticated stage with relationships between outcome goals in business terms, and it-process improvement measures now well understood. Real results have been communicated to management in the form of a balanced scorecard. • The enterprise's management team is now working together for the common goal of maximizing it-value delivery and managing it-related risks. There have been regular assessments of it-capabilities and projects have been completed that have delivered real improvements to it's performance. • Relationships among the it-function, its users in the business community and external service providers are now based on service definitions and service agreements.
5	<p>Optimized</p> <ul style="list-style-type: none"> • The it-governance practices have developed into a sophisticated approach using effective and efficient techniques. There is true transparency of it-activities, and the board feels in control of the it-strategy. • It-activities have been optimally directed toward real business priorities, and the value being delivered to the enterprise can be measured and steps taken on a timely basis to correct significant deviations or problems. • The balanced scorecard approach has evolved into one that is focused on the most important measures relevant to the enterprise's overall business strategy. The effort spent on risk management (and on it-management activities generally) has been streamlined through adoption of standardized and, where possible, automated processes. • The practice of continuous improvement of it-capability is embedded in the culture and this includes regular external benchmarking and independent audits providing positive assurance to management. • Overall, the cost of it is monitored effectively and the organization is able to achieve optimal it spending through continuous internal improvements, the effective outsourcing of selected services and effective negotiation with vendors. When dealing with external business partners or service providers, the organization is able to demonstrate first-class performance and demand best practices from others.

Tabel 2. Kilde: Control Objectives for Information and related Technology (COBIT)

5. Er I klar?

Vejen frem – tjeklisten for en god start på compliance

Som afslutning på denne artikel vil jeg give nogle erfaringer videre, som kan være nyttige:

Start med udgangspunktet – hvor meget kontrollerer I allerede i dag?

- Definer projektets omfang.
- Sørg for ledelsens deltagelse eller involvering.

- Foretag en *pragmatisk* risikovurdering – og dokumenter de vigtige processer.
- Koncentrér kontroller om *forretningskritiske* områder - og arbejd ud fra det.
- Overvej om koordineringen skal varetages af én person, eller om det er en risiko.
- Tag højde for, at kravene kan variere på forskellige lokationer.
- PAS PÅ IKKE AT LÆGGE FOR HÅRDT UD.

Der er både fornuft og forretningen i at dokumentere arbejdsprocesser og regler, men det er vigtigt at gøre det i et tempo, hvor alle kan følge med, og det behøver ikke at være kedeligt. God kvalitet har altid været et konkurrenceparameter – og er det stadig. At man også opnår compliance ved at have ensartet kvalitet og veldokumenteret opfølgning, kan betragtes som et ekstra plus.

God fornøjelse.

6. Om forfatteren – Frederik Helweg-Larsen

Af hovedredaktør Ulf Munkedal

Frederik Helweg-Larsen er direktør og stifter af Policy Enforcer ApS, der er en dansk virksomhed delvist ejet af Teknologisk Innovation A/S og Ministeriet for Videnskab, Teknologi og Udvikling. Selskabet udvikler software til systematisk formulering, vedligeholdelse og efterlevelse af politikker - med særlig fokus på it-sikkerhed og kvalitetssikring. Frederik har arbejdet med sikkerhed siden 1992 og har tidligere været direktør for Swanholm Distribution A/S, leder af kompetencecenter for IT-sikkerhed i WM-data A/S samt direktør og stifter af Netsecure Danmark A/S.

Læs mere om Policy Enforcer på: www.policyenforcer.dk

