KREDITTILSYNET
The Financial Supervisory Authority of Norway

VEILEDNING I ETTERLEVELSE AV IKT-FORSKRIFTEN FOR MINDRE SPAREBANKER

INNLEDNING

Høsten 2006 laget Kredittilsynet en veiledning i etterlevelse av IKT-forskriften spesielt rettet mot mindre foretak. Dette var på bakgrunn av signaler om at mange små foretak synes det er vanskelig å vite hvordan de kan etterleve forskriften fordi foretaket er lite, med begrenset IT-virksomhet og forskriften i utgangspunktet virker omfattende. Veiledningen tok utgangspunkt i et lite eiendomsmeglerforetak og var formulert som et eksempel på hvordan et foretak kan sikre at det etterlever forskriften.

Kredittilsynet fikk i etterkant av denne utgivelsen en forespørsel fra Sparebankforeningen om å lage en veiledning for de mindre sparebankene. Kredittilsynet har nå laget en slik veiledning spesielt rettet mot mindre sparebanker. Også denne gangen er veiledningen formet som et eksempel på hvordan et fiktivt foretak kan sikre at det etterlever IKT-forskriften, nemlig sparebanken BankBukkeneBruse.

Felles for mindre sparebanker i Norge er at IT-virksomheten i stor grad er utkontraktert til en ekstern IT-leverandør. IT-leverandøren er gjerne et større selskap som leverer IT-tjenester til flere banker. Mange mindre sparebanker i Norge har valgt å inngå i et fellesskap med andre sparebanker med en felles IT-leverandør. Avtalene om IT-tjenester gjøres ofte mellom en representant for samarbeidet og IT-leverandøren og ikke mellom banken og IT-leverandøren direkte. Modellen kan være effektiv og rasjonell. Den enkelte bank behøver ikke ta stilling til kompliserte teknologiske vurderinger og avtalemessige detaljer. Samtidig kan resultatet bli at den enkelte sparebank blir stående fjernt fra der beslutningene tas. Spesielt de mindre sparebankene kan oppleve dette fordi de har mindre påvirkningskraft i sparebankfellesskapet og i mindre grad er premissgiver for utviklingen av IT-systemene enn de større sparebankene. Dette og flere tilsvarende forhold kan gjøre det vanskelig for en mindre bank å stille krav til leverandørene og kontrollere IT-leveransene. Likevel fritar ikke dette den enkelte bank fra ansvaret for IT-løsningene og å oppfylle myndighetskravene.

I denne veiledningen viser vi et eksempel på hvordan en mindre sparebank dokumenterer sin etterlevelse av IKT-forskriften. Kredittilsynet ønsker å understreke sparebankenes eget ansvar for IT-tjenestene. Veiledningen kan være en hjelp til sparebankene i å oppfylle myndighetskrav, men kan forhåpentligvis også bidra til å gjøre de mindre sparebankene tryggere i rollen som styrer, bestiller og kontrollør av IT-leveransene.

EKSEMPEL PÅ HVORDAN EN MINDRE SPAREBANK KAN ETTERLEVE IKT-FORSKRIFTEN

Presentasjon av sparebanken BankBukkeneBruse og IT-virksomheten i banken.

Sparebanken BankBukkeneBruse er en mindre sparebank som ble etablert i et tradisjonsrikt norsk bygdesamfunn i januar 1955. Banken betjener personmarkedet og den lokale næringsvirksomheten i bygda. Banken har 19 stillinger fordelt på hovedkontoret og en filial.

BankBukkeneBruse er med i en sammenslutning av sparebanker; SpareBankKompaniet. SpareBankKompaniet har inngått avtale med IT-leverandøren ComputerAssistent om drift og videreutvikling av kjerneløsningen til sparebankene. ComputerAssistent leverer i tillegg en del andre IT-løsninger. SpareBankKompaniet har også avtaler med andre leverandører om ulike IT-løsninger. Den enkelte bank i sammenslutningen gjør ingen direkte avtaler med IT-leverandører. Alle avtaler inngås gjennom SpareBankKompaniet.

Siden ingen forretningsapplikasjoner utvikles eller driftes av banken, er bankens egen IT-virksomhet begrenset. IT-organisasjonen i sparebanken BankBukkeneBruse består av to personer; IT-leder Marit og IT driftsansvarlig Gjermund. Marit er bindeleddet mellom forretningssiden i banken og IT-systemene og har ansvar for oppfølging av oppdrag og avtaler mot SpareBankKompaniet. Gjermund er ansvarlig for drift og vedlikehold av nettverk, lokalt installert programvare, servere og PC'er. Både Marit og Gjermund har direkte kontakt med ComputerAssistent om driftsmessige forhold. Banksjefen i BankBukkeneBruse, Ragnhild, har det øverste ansvaret for IT-virksomheten på lik linje med ansvar for øvrig virksomhet i banken. Knut er assisterende banksjef. Alle viktige beslutninger i IT-virksomheten er forankret hos ledelsen i banken.

Porteføljen av IT-utstyr i banken består av 20 stasjonære arbeidsstasjoner hvorav 15 på hovedkontoret og fem i filialen. I tillegg har banken ti bærbare PC'er. Enkelte ansatte har fått tildelt en fast bærbar PC til bruk utenfor kontoret mens fem av de bærbare PC'ene lånes ut på bestilling. Foretaket har en filserver, en server for programvare, tre printere og en skanner. Arbeidsstasjonene og serverne er koblet i et lokalt nettverk. Det er installert et ekstranett mellom ComputerAssistent og BankBukkeneBruse og et intranett mellom SpareBankKompaniet og BankBukkeneBruse. Som beskyttelse mellom lokalt nettverk og ekstranett, intranett og internett er det installert rutere med brannmurprogramvare. Både de stasjonære og de bærbare PC'ene har installert standard kontorstøttesystemer. Forretningsspesifikke applikasjoner driftes av IT-leverandøren med sentral lagring av applikasjoner og data. Dette gjelder både kjerneløsningen, back office applikasjonene som brukes av de ansatte i banken og de webbaserte selvbetjeningskanalene. Banken har tre minibanker.; en inne i hovedkontoret, en utenfor hovedkontoret og en utenfor filialen. Banken har ansvar for første linje brukerstøtte på drift av minibankene.

Foretakets dokumentasjon av hvordan de etterlever IKT-forskriften

Sparebanken BankBukkeneBruse har prioritert å bygge opp noe kompetanse på internasjonale rammeverk for IT-organisering som ITIL og CobiT. Marit har tatt et tre dagers ITIL-kurs og er ITIL Foundation sertifisert. Gjermund og Marit har gjennom ukentlige samlinger våren og høsten 2006 gjennomgått de 34 CobiT prosessene samt gjort seg kjent med Kredittilsynets temamodul med kontrollspørsmål knyttet til de 34 prosessene (http://www.kredittilsynet.no/wbch3.exe?ce=15430). Banken har valgt å bruke elementer fra disse rammeverkene når de har organisert og dokumentert IT-virksomheten. Dette er også i tråd med IKT-forskriften som gjennom de 13 paragrafene støtter en metodisk prosesstilnærming til organisering av IT-virksomheten. BankBukkeneBruse har besluttet å lage en dokumentasjon av IT-virksomheten hvor det under hvert kapittel er referanser til paragrafer i IKT-forskriften. På den måten kan banken dokumentere at det har blitt gjort en gjennomgang av forskriften samtidig som banken kan vise til dokumenterte vurderinger og rutiner for de ulike områdene av IT-virksomheten. I dokumentasjonen refereres det til aktuelle maler og skjemaer som brukes for å operasjonalisere rutinene.

Nedenfor gjengir vi "Dokumentasjon av IT-virksomheten i sparebanken BankBukkeneBruse". Maler og skjemaer det refereres til, er i varierende grad inkludert. Dette er med hensikt fordi dette ikke er ment å være en oppskrift, men heller et eksempel som kan gi ideer og innspill til mindre sparebanker i arbeidet med å sikre og dokumentere IT-virksomheten og etterleve IKT-forskriften.

Dokumentasjon av IT-virksomheten i sparebanken BankBukkeneBruse

En eksemplifisert veiledning i etterlevelse av IKT-forskriften for mindre sparebanker

Innholdsfortegnelse

Revisjonshistorikk

Versjonsnr.	Dato	Beskrivelse av endring	Signatur
1.0	20.01.2006	Godkjent versjon	MAR
1.1	17.03.2006	Oppdatert etter gjennomført ROS-analyse 2006	MAR
1.2	27.04.2007	Oppdatert etter gjennomført ROS-analyse 2007. Supplert kap.1	MAR

Kapittel 1: IT-strategi for BankBukkeneBruse for perioden 2006 - 2008

Ref. IKT-forskriftens §§ 2 Planlegging og organisering og 12 Utkontraktering

§ 2 Planlegging og organisering

Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.

Ved utkontraktering av deler eller hele IKT-virksomheten skal foretaket ha egne retningslinjer som skal sikre leveransen.

Det skal oppnevnes en ansvarlig i foretaket for de ulike deler av IKT-virksomheten. Med ansvarlig menes en funksjon eller stilling.

§ 12 Utkontraktering

Foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å inspisere og kontrollere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon.

Avtalen skal videre sikre at Kredittilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Kredittilsynet finner det nødvendig som et ledd i tilsynet med foretaket.

Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen.

BankBukkeneBruse har en IT-strategi med et treårsperspektiv. Nåværende IT-strategi gjelder for perioden 2006 – 2008.

Forretningsstrategi

Sparebanken BankBukkeneBruse er en lokal sparebank som skal betjene bygdas innbyggere og næringsliv med innlån og utlån og tilby andre finansielle tjenester som forsikring, pensjon og verdipapirhandel. Banken tar ikke mål av seg å vokse mer enn ca 15 % i strategiperioden i forhold til størrelsen i dag. Bankens historie går tilbake til 1955, og banken har i hele denne perioden vært en sentral aktør i lokalmiljøet. Dette ønsker banken å fortsette å være. For å konkurrere med de store bankene, må banken kunne tilby tjenester med høy kvalitet til konkurransemessige priser. Dette mener BankBukkeneBruse å klare blant annet ved å minimalisere marginene. Det er ikke et mål for banken å akkumulere overskudd, men bidra til et rikere liv for bygdas innbyggere. Mellom 10 og 25 % av bankens overskudd skal tilbakeføres til lokalmiljøet gjennom støtte til tiltak i lokale organisasjoner, foreninger og arrangementer. Sparebanken BankBukkeneBruse skal være en bank kundene kan stole på, en bank kundene kan kommunisere med og en bank kundene kan få forståelige og fornuftige svar fra når de spør. I dette inngår høy kvalitet på IT-systemer og brukerstøtteapparat.

Bankens historie sett i et IT-perspektiv

BankBukkeneBruse ble etablert som sparebank lenge før EDB var et tilgjengelig verktøy i operasjonen av banktjenestene. Banken har gradvis tilpasset seg tidens krav til bruk av EDB. Fra midten av åttitallet har banken benyttet en sentralisert IT-løsning for

kjernesystemene. Fram til slutten av nittitallet hadde banken selv hånd om oppgradering av en del av systemporteføljen og lagring av forretningsdata lokalt. Ny teknologi og større krav til IT-systemer og selvbetjeningskanaler, gjorde at BankBukkeneBruse i 2001 bestemte å slutte seg til SpareBankKompaniet og basere seg på de IT-løsninger SpareBankKompaniet har valgt for de tilsluttede sparebankene. Etter dette er bankens egen IT-virksomhet redusert og består i dag av ansvar for kontorstøtteapplikasjoner og sikkerhetsapplikasjoner, drift av lokalt nettverk og lokale maskiner, samt oppfølging av avtaler med og leveranser fra samarbeidspartner og leverandører. Utviklingen har medført at det pr i dag er vanskeligere å opprettholde IT-kompetanse i banken enn det var i den perioden banken hadde en større del av ansvaret for IT-virksomheten selv.

Forankring av IT-virksomheten på ledelsesnivå
Sparebanken BankBukkeneBruse har vurdert IT-virksomheten som en vesentlig faktor for at banken skal nå forretningsmessige mål. IT har blitt en stadig viktigere del av tjenesteleveransene, og det er i dag umulig å tenke seg drift av banken uten bruk av IT. Samarbeidet med andre banker gjennom tilslutning til SpareBankKompaniet åpner muligheten for at BankBukkeneBruse kan tilby tilnærmet samme portefølje av IT-baserte tjenester som de større bankene. Samtidig har reduksjonen i bankens egen operasjonelle IT-virksomhet skapt nye utfordringer når det gjelder å opprettholde tilstrekkelig kompetanse på IT-området. Kompetanse er nødvendig for å kunne formulere velbegrunnede ønsker om endringer og å kunne styre og kontrollere IT-leveransene. Banken har på denne bakgrunn en strategisk målsetting om å opprettholde et høyt nivå på bankens samlede IT-kompetanse. Høy oppmerksomhet om IT-virksomheten på ledelsesnivå skal bidra til dette. Alle viktige beslutninger vedrørende IT-virksomheten skal fattes på øverste ledernivå, og IT-leder skal rapportere månedlig til bankens ledelse om status på IT-virksomheten. Bankens ledelse blir innkalt til alle møter med SpareBankKompaniet og andre aktuelle samarbeidspartnere på IT-siden og skal tilstrebe å møte på minimum halvparten av disse.

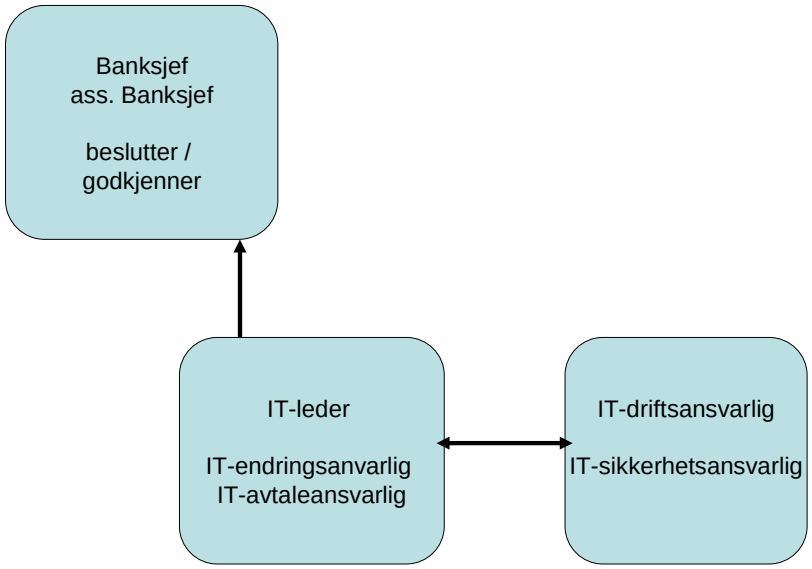
IT-kompetanse
BankBukkeneBruse har vurdert det som viktig å opprettholde høy kompetanse på IT-siden til tross for at bankens egen IT-virksomhet er begrenset. På den måten kan banken bedre følge opp kvaliteten på IT-leveransene og stille begrunnede krav til leverandørene både hva gjelder kvaliteten på løpende tjenester og bestilling av nye tjenester.

BankBukkeneBruse har valgt å basere organisering av IT-virksomheten på elementer fra de internasjonale rammeverkene ITIL og CobiT. IT-leder og IT-driftsansvarlig skal ha oppdatert kjennskap til disse. IT-personalet skal minimum ha fem dager med kompetansefremmende kurs hvert år.

Som et ledd i å sikre kompetente medarbeidere med lokal forankring, har banken bestemt å utlyse et stipend hvert annet år. Stipendet er på kr. 100.000 til utdannelse innen IT med krav til 1 års plikttjeneste i banken etter endt utdannelse. En forutsetning for å søke stipendet er minst 10 års botid i kommunen. Banken vurderer dette som et positivt tiltak fra bankens side for å få tilgang til oppdatert IT-kompetanse. Det skal utarbeides et

program for pliktkandidaten med vekt på en toveis kompetanseoverføring mellom de fast ansatte i IT-organisasjonen i banken og pliktkandidaten.

Rollefordeling i IT-virksomheten
På tross av bankens begrensede ressurser på IT-siden har banken vurdert det som viktig å organisere IT-virksomheten med en formalisert rolleinndeling for å klargjøre ansvarsforholdene. Banken har definert disse rollene i IT-virksomheten: **IT-leder, IT-driftsansvarlig**, IT-sikkerhetsansvarlig, IT-avtaleansvarlig og IT-endringsansvarlig. Bankens begrensede ressurser på IT-siden gjør at samme person må ikles flere roller. Rollen som IT-leder består først og fremst i å påføre den formelle godkjenningen på endringer og oppgraderinger i IT-systemene samt være IT-virksomhetens representant utad mot leverandør og samarbeidspartner. IT-driftsansvarlig er p.t. også tillagt ansvar for IT-sikkerhet. Bankens ledelse har en rolle som øverste ansvarlig for beslutninger knyttet til IT-virksomheten. Slik ser organisasjonskartet ut:



Ved sykdom eller annet fravær fungerer IT-leder og IT-driftsansvarlig som gjensidige stedfortredere for hverandre.

Lokal IT-virksomhet
Banken har ansvar for drift av lokalt nettverk, arbeidsstasjoner og bærbare PC'er samt filserver og server for programvare. Banken forestår oppgraderinger av operativsystem, kontorstøtteprodukter og sikkerhetsprodukter på lokale maskiner. I tillegg til dette oppdaterer banken kodedata for parametersetting i forretningsapplikasjonene som kommuniseres gjennom filoverføring til ComputerAssistent. Banken har begrenset driftsansvar for minibankene.

Utkontraktering av IT-virksomhet

BankBukkeneBruse utvikler ikke IT-systemer og drifter heller ikke de forretningsspesifikke applikasjonene. Banken gjør ingen avtaler direkte med IT-leverandører. Gjennom avtalen BankBukkeneBruse har med SpareBankKompaniet om deltakelse i sammenslutningen, baserer banken seg på de avtaler om utkontraktering av IT-operasjonene SpareBankKompaniet gjør på vegne av bankene. SpareBankKompaniet inngår rammeavtaler for driften, og i disse inngår spesifiserte SLA-avtaler for den enkelte bank. Banken kan til en viss grad plukke fra den pakken med IT-løsninger SpareBankKompaniet tilbyr. Det er avtalefestet månedlige møter mellom SpareBankKompaniet og banken. IT-leder deltar alltid på disse, bankens ledelse kalles inn på alle møter og deltar på minimum halvparten av møtene.

Deltagelse i IT-brukerforum
BankBukkeneBruse vurderer det som viktig å delta i IT-brukerforumet for banker tilsluttet SpareBankKompaniet. Brukerforumet gir mulighet for større kraft bak felles ønsker om endrede løsninger og skjerping av krav til IT-leverandøren eller SpareBankKompaniet. BankBukkeneBruse skal aktivt bidra til å opprettholde et levende og engasjert brukerforum på fylkesnivå samt delta i den årlige brukerkonferansen på nasjonalt nivå.

Valg av IT-leverandør
BankBukkeneBruse har gjennom tilslutning til SpareBankKompaniet liten påvirkningskraft på valg av IT-leverandør utover et visst spillerom i forhold til valg av applikasjoner / IT-tjenester banken vil ta i bruk. Banken har vurdert at den p.t. ikke har ressurser til å stå alene uten knytning til en banksammenslutning. Samtidig har banken besluttet å gjøre en regelmessig evaluering av nettopp dette forholdet. Enkelte sparebanker i Norge er ennå frittstående og gjør avtaler direkte med IT-leverandører. Banken vil hvert tredje år innhente priser som gjør det mulig å estimere kostnadsdifferansen mellom å inngå avtaler direkte med en IT-leverandør og avgiften til SpareBankKompaniet. Det er IT-leders ansvar å legge fram et kostnadsestimat samt en overordnet risikovurdering i forhold til å trekke seg ut av SpareBankKompaniet. Resultatet av dette arbeidet legges ditto fram for bankens styre sammen med internkontrollrapporten og IT-risikoanalysen.

Nettsted på Internettet
www.BankBukkeneBruse.no er bankens nettsted på internettet. Her får kundene tilgang til selvbetjeningsløsninger blant annet nettbanken. Informasjonen på www.BankBukkeneBruse.no skal reflektere bankens profil med vekt på bankens lokale tilhørighet.

Operasjonalisering av prosesser og rutiner
BankBukkeneBruse har laget skjemaer i excel for å følge opp IT-virksomheten. Banken vurderer dette som et tilstrekkelig verktøy for å formalisere og operasjonalisere IT-prosessene, også i forhold til å imøtekomme en økning i aktiviteten.

Etterlevelse av lover og regler

BankBukkeneBruse har konsesjon fra Kredittilsynet og er underlagt IKT-forskriften. For å sikre regelmessig vurdering av om interne retningslinjer og rutiner for IT-virksomheten og IKT-forskriften etterleves, skal denne dokumentasjonen gjennomgå en årlig evaluering. Det skal kvitteres for gjennomført evaluering i tabellen for versjonshåndtering på side 2.

Kapittel 2: Risikoanalyse

Ref. IKT-forskriftens § 3 Risikoanalyse

> ***§ 3 Risikoanalyse***
>
> *Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene.*
> *Foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten. Prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen.*
>
> *Foretaket skal minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.*

Sparebanken BankBukkeneBruse vurderer gjennomføring av risikoanalyse for foretakets IT-virksomhet som et viktig bidrag til å nå bankens mål om å levere tjenester med en sikkerhet og tilgjengelighet som er i tråd med det banken garanterer kundene.

Årlig risikoanalyse av IT-virksomheten
Banken skal gjennomføre en årlig risikoanalyse av IT-virksomheten med framlegging av resultatet for ledelsen innen 31.03. Resultatet av risikoanalysen skal legges ved den årlige internkontrollrapporten til styret. Risikoen som avdekkes gjennom analysen sammen med tiltakene som spesifiseres, skal gi en situasjon der det totale risikobildet på IT-området er innenfor akseptable grenser. Risikoanalysen skal være datert og signert, og denne signaturen er en bekreftelse på at risikoen er vurdert som akseptabel.

Risikoanalyse ved IT-prosjekt og større endringer
Ved større endringer og oppgaver i tilknytning til IT-virksomheten som bestemmes løst gjennom en prosjektorganisering, skal en risikoanalyse av IT-oppgavene inngå som et element i den innledende fasen.

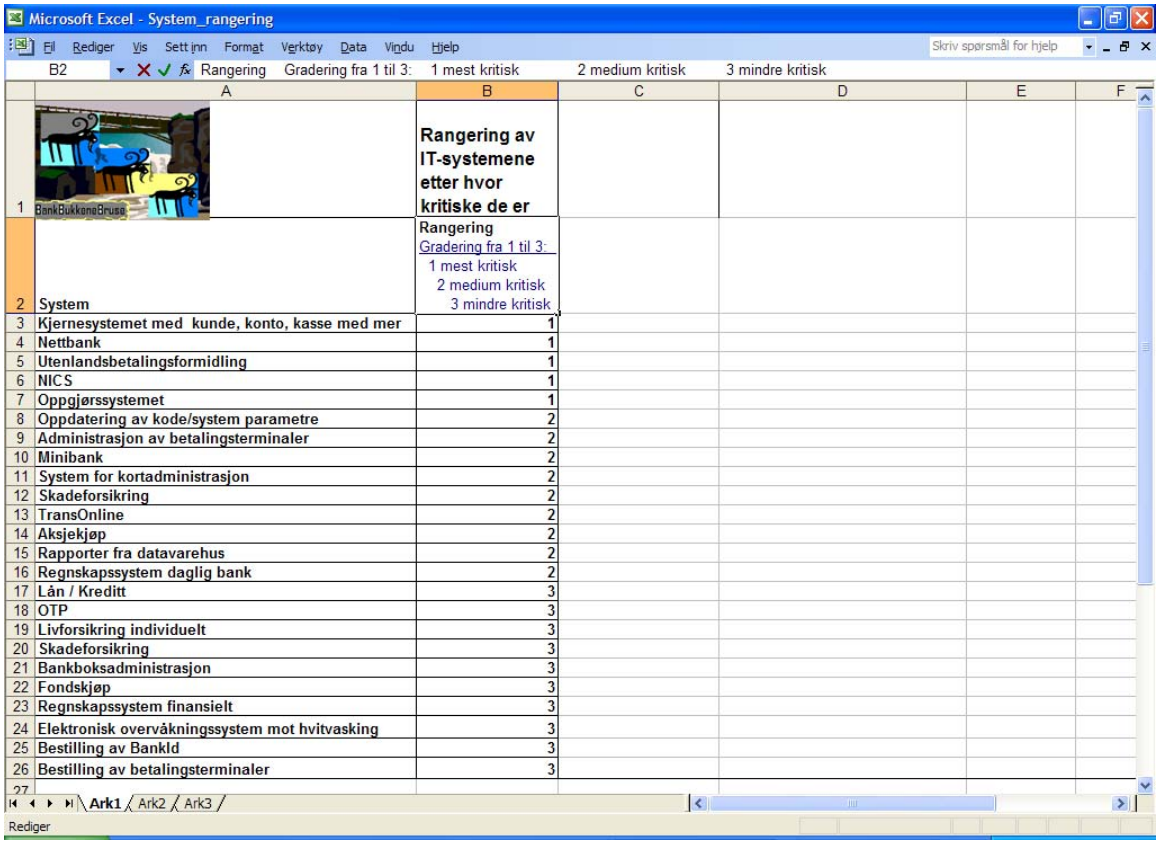
Forankring og deltagelse i gjennomføring av risikoanalysen
Siden bankens forretningsvirksomhet i så stor grad er basert på bruk av IT-systemer med operasjonell risiko hvis IT-systemene svikter, skal risikoanalysen av IT-virksomheten forankres hos den øverste ledelsen og styret i banken. Dette er i tråd med bankens strategi og et krav i internkontroll-forskriften. IT-leder er ansvarlig for selve gjennomføringen og dokumenteringen av risikoanalysen. Aktuelle ressurser fra forretningssiden deltar i gjennomføringen. Risikoanalysen godkjennes og undertegnes av banksjef samt av IT-leder og IT-driftsansvarlig.

Bankens valg av metode for risikoanalyse av IT-virksomheten
BankBukkeneBruse har vurdert ulike måter å gjennomføre risikoanalysen på. Som bakgrunnsstoff har banken blant annet lest kapitel 5 ”Hvordan gjennomføre risikoanalyser av IKT-systemer” i sluttrapport fra prosjektet
Beskyttelse av samfunnet 5 (BAS5) – Sårbarhet i kritiske IKT-systemer som er lagt ut på internett på http://rapporter.ffi.no/rapporter/2007/01204.pdf
samt konferert ISO standard 27005 ”Information security risk management”.

Rangering av systemer etter hvor kritiske de er
BankBukkeneBruse har laget en rangering av IT-systemene etter hvor kritiske systemene er for banken. Et IT-system er i denne sammenheng definert som summen av funksjonalitet og data. Rangeringen gir input både til risikoanalysen og til kontinuitets- og katastrofeløsningene i banken. Systemene er gradert på en skala fra 1 til 3 hvor systemer gradert til 1 er de mest kritiske. Graderingen er i første omgang gjort i forhold til krav til tilgjengelighet der systemene blir målt på hva som er akseptabel tid systemet kan være ute av funksjon og akseptabelt tap av data. Banken har også trukket inn sikkerhetsperspektivet som et tilleggskriterium for rangeringen dvs. hvor kritiske systemene er med hensyn på brudd på konfidensialitet og / eller integritet. Dette gjør rangeringen mer kompleks, men banken ser at det hovedsaklig er sammenfallende utslag både på krav til tilgjengelighet og krav til sikkerhet med hensyn på beskyttelse av konfidensialitet og integritet. Banken har derfor valgt en enkelt rangering fra 1 til 3 der gradene er definert slik:

> *1: mest kritisk:*
> Akseptabelt bortfall av tjenesten er definert til 2 timer og ikke noe tap av data
> *2: medium kritisk:*
> Akseptabelt bortfall av tjenesten er definert til 1 dag og tap av data til en dags produksjon
> *3: minst kritisk:*
> Akseptabelt bortfall av tjenesten er definert til 1 uke og tap av data tilsvarende fem dagers produksjon

Slik ser oppdatert rangering av systemene ut:



Microsoft Excel - System_rangering

Fil Rediger Vis Sett inn Format Verktøy Data Vindu Hjelp — Skriv spørsmål for hjelp

B2 | Rangering | Gradering fra 1 til 3: | 1 mest kritisk | 2 medium kritisk | 3 mindre kritisk

	A	B	C	D	E	F
1	BankBukkeneBruse	**Rangering av IT-systemene etter hvor kritiske de er**				
2	System	Rangering Gradering fra 1 til 3: 1 mest kritisk 2 medium kritisk 3 mindre kritisk				
3	Kjernesystemet med kunde, konto, kasse med mer	1				
4	Nettbank	1				
5	Utenlandsbetalingsformidling	1				
6	NICS	1				
7	Oppgjørssystemet	1				
8	Oppdatering av kode/system parametre	2				
9	Administrasjon av betalingsterminaler	2				
10	Minibank	2				
11	System for kortadministrasjon	2				
12	Skadeforsikring	2				
13	TransOnline	2				
14	Aksjekjøp	2				
15	Rapporter fra datavarehus	2				
16	Regnskapssystem daglig bank	2				
17	Lån / Kreditt	3				
18	OTP	3				
19	Livforsikring individuelt	3				
20	Skadeforsikring	3				
21	Bankboksadministrasjon	3				
22	Fondskjøp	3				
23	Regnskapssystem finansielt	3				
24	Elektronisk overvåkningssystem mot hvitvasking	3				
25	Bestilling av BankId	3				
26	Bestilling av betalingsterminaler	3				
27						

Ark1 Ark2 Ark3

Rediger

Rangeringen av systemene etter hvor kritiske de er danner bakteppe for risikoanalysen. BankBukkeneBruse vurderer mulige trusler og uønskede hendelser i lys av dette. Banken har valgt en enkel rangering av identifiserte risikoer etter alvorlighetsgrad høy, middels eller lav. Denne rangeringen er basert på produktet av sannsynligheten for at hendelsen vil oppstå og konsekvens av hendelsen. For å vurdere sannsynligheten for at en hendelse kan oppstå, har banken blant annet benyttet historiske data. Banken har videre vurdert tiltak for å redusere risikoen. Gjenværende risiko er rangert, etter samme skala, til høy, middels eller lav.

Med bakgrunn i at bankens lokale IT-virksomhet er begrenset, mens systemporteføljen administreres av SpareBankKompaniet og driftes og utvikles av ulike IT-leverandører, har banken valgt å dele identifiserte risikoer i tre grupper:

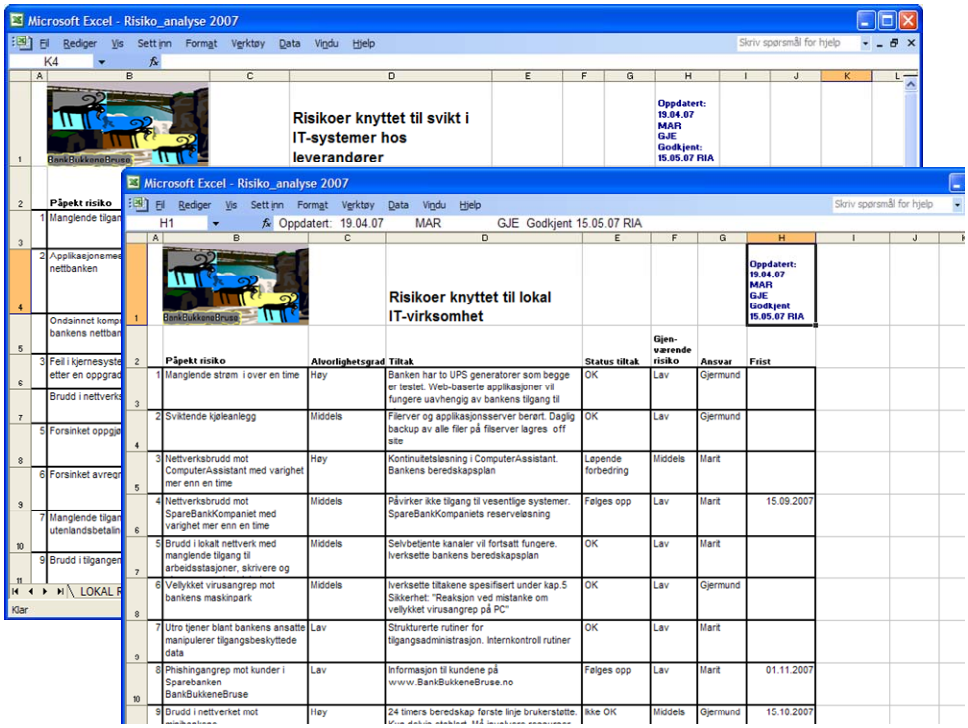
- Risikoer knyttet til lokal IT-virksomhet
- Risikoer knyttet til svikt i IT-systemer hos leverandører
- Risikoer knyttet til organisering av IT-virksomheten

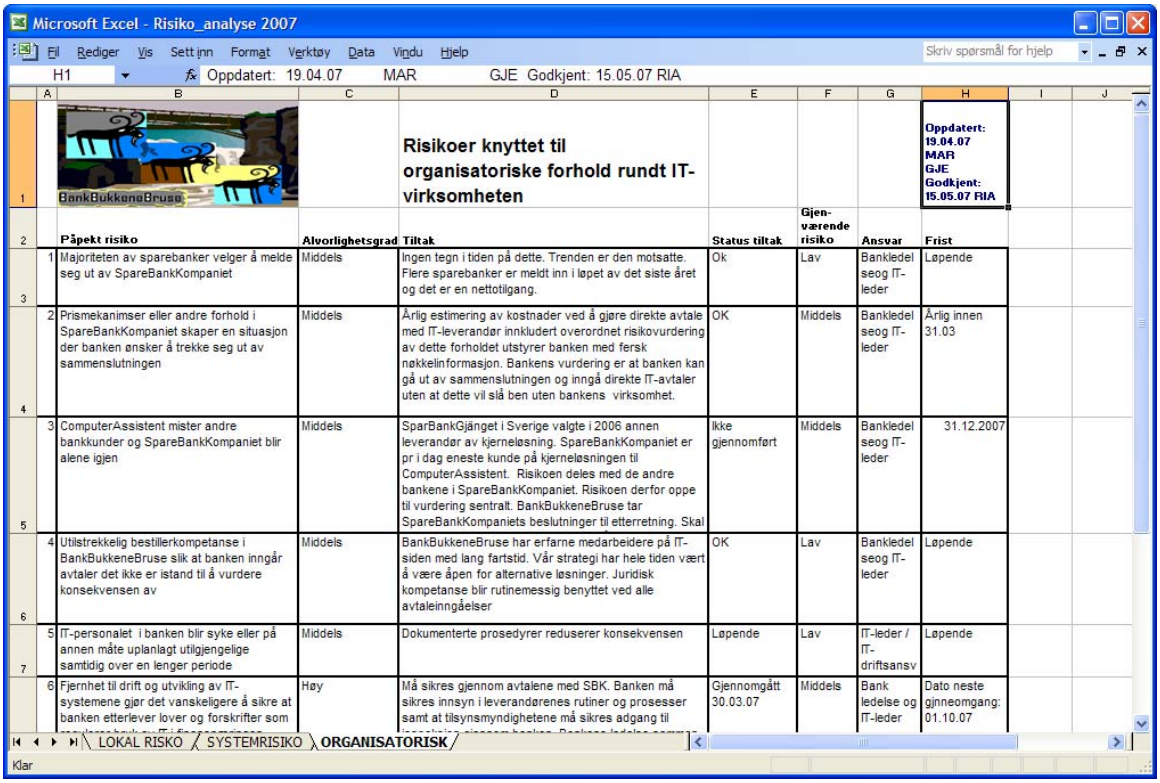
Dybdeanalyse på utvalgte områder.

For BankBukkeneBruse er nettbanken kategorisert til å være et av de mest kritiske systemene for banken. Bakgrunnen for dette er at nær 90 % av betalingstransaksjonene passerer gjennom denne kanalen, kanalen er selvbetjent og den har ubrutt åpningstid. I en krisesituasjon vil banken kunne betjene viktige betalingsoppdrag gjennom andre kanaler,

men banken har ikke ressurser til å erstatte nettbanken verken med hensyn til volum eller tilgjengelighet gjennom andre betalingskanaler. Nettbankløsningen er utviklet av en tredjepartsleverandør til SpareBankKompaniet. I IT-brukerforums landsmøte 2006 ble det besluttet at bankene i fellesskap vil bruke ressurser på å få gjennomført en dyptgående risikoanalyse av nettbankløsningen. Bankene har engasjert et forskningsmiljø til å bistå i å evaluere leverandørens risikoanalyse samt vurdere mulige scenarier i dag og i morgen knyttet til nettbankens tilgjengelighet (stabilitet), brukervennlighet og sikkerhet. BankBukkeneBruse vil bringe resultatet av denne analysen inn som en del av underlaget for egen risikoanalyse.

Banken har laget en mal i Excel for risikoanalysen. Her er utdrag av risikoanalysen for 2007:





	Påpekt risiko	Alvorlighetsgrad	Tiltak	Status tiltak	Gjen-værende risiko	Ansvar	Frist
1	Majoriteten av sparebanker velger å melde seg ut av SpareBankKompaniet	Middels	Ingen tegn i tiden på dette. Trenden er den motsatte. Flere sparebanker er meldt inn i løpet av det siste året og det er en nettotilgang.	Ok	Lav	Bankledel seog IT-leder	Løpende
2	Prismekanismer eller andre forhold i SpareBankKompaniet skaper en situasjon der banken ønsker å trekke seg ut av sammenslutningen	Middels	Årlig estimering av kostnader ved å gjøre direkte avtale med IT-leverandør innkludert overordnet risikovurdering av dette forholdet utstyrer banken med fersk nøkkelinformasjon. Bankens vurdering er at banken kan gå ut av sammenslutningen og inngå direkte IT-avtaler uten at dette vil slå ben uten bankens virksomhet.	OK	Middels	Bankledel seog IT-leder	Årlig innen 31.03
3	ComputerAssistent mister andre bankkunder og SpareBankKompaniet blir alene igjen	Middels	SparBankGjänget i Sverige valgte i 2006 annen leverandør av kjerneløsning. SpareBankKompaniet er pr i dag eneste kunde på kjerneløsningen til ComputerAssistent. Risikoen deles med de andre bankene i SpareBankKompaniet. Risikoen derfor oppe til vurdering sentralt. BankBukkeneBruse tar SpareBankKompaniets beslutninger til etterretning. Skal	Ikke gjennomført	Middels	Bankledel seog IT-leder	31.12.2007
4	Utilstrekkelig bestillerkompetanse i BankBukkeneBruse slik at banken inngår avtaler det ikke er istand til å vurdere konsekvensen av	Middels	BankBukkeneBruse har erfarne medarbeidere på IT-siden med lang fartstid. Vår strategi har hele tiden vært å være åpen for alternative løsninger. Juridisk kompetanse blir rutinemessig benyttet ved alle avtaleinngåelser	OK	Lav	Bankledel seog IT-leder	Løpende
5	IT-personalet i banken blir syke eller på annen måte uplanlagt utilgjengelige samtidig over en lenger periode	Middels	Dokumenterte prosedyrer reduserer konsekvensen	Løpende	Lav	IT-leder / IT-driftsansv	Løpende
6	Fjernhet til drift og utvikling av IT-systemene gjør det vanskeligere å sikre at banken etterlever lover og forskrifter som	Høy	Må sikres gjennom avtalene med SBK. Banken må sikres innsyn i leverandørenes rutiner og prosesser samt at tilsynsmyndighetene må sikres adgang til	Gjennomgått 30.03.07	Middels	Bank ledelse og IT-leder	Dato neste gjnneomgang: 01.10.07

Kapittel 3: Kvalitet

Ref. IKT-forskriftens § 4. Kvalitet

> ***§ 4 Kvalitet***
>
> *Foretaket skal fastsette kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot foretakets øvrige mål. Foretaket skal ha dokumenterte prosedyrer for oppfølging av fastsatte kvalitetsmål.*

For BankBukkeneBruse betyr kvalitet i IT-virksomheten

- at tjenester er tilgjengelige i de tidsrom banken tilbyr tjenestene
- at tjenestene utføres korrekt med riktig beregnede verdier
- at tjenestene ivaretar kundens krav til konfidensialitet om egne data
- at banken tilbyr et utvalg IT-tjenester som er i tråd med best practice på bankområdet

Kvalitetsmål
BankBukkeneBruse har definert følgende konkrete kvalitetsmål for IT-virksomheten:

- tjenester gjennom selvbetjeningskanalen på www.BankBukkeneBruse.no skal være tilgjengelige 24 / 7 med unntak for avtalte servicevinduer
- minibankene skal være tilgjengelige 24 / 7
- IT-systemer bankens ansatte benytter skal være tilgjengelige i arbeidstiden fra kl. 08.00 til 16.00
- IT-systemene skal ikke inneholde feil etter oppgraderinger og versjonsendringer
- IT-systemene skal ha sikkerhetsbeskyttelse på et nivå som gjør at ondsinnede angrep mot systemer og data ikke lykkes
- Banken skal håndtere IT-virksomheten i samsvar med bankens interne regelverk og prosedyrer som følger av denne dokumentasjonen og gjennom dette etterleve lov og forskrifter.

Virkemidler for å nå kvalitetsmålene
Kvalitet er et område BankBukkeneBruse vier høy oppmerksomhet. Dette gjelder ikke bare på IT-siden, men gjelder generelt for bankens arbeid og er et ankerfeste i bankens generelle forretningsstrategi. BankBukkeneBruse skal være en bank kundene kan stole på, en bank kundene kan kommunisere med og en bank kundene kan få forståelige og fornuftige svar fra når de spør. Kvalitet er ikke noe banken blir ferdig med. Det er en pågående prosess som ikke skal hvile.

BankBukkeneBruse vurderer veldefinerte prosesser og rutiner som et viktig ledd i å nå kvalitetsmålene på IT-siden. Dokumenterte prosesser (gjennom dette dokumentet) støttet av detaljerte rutinebeskrivelser og skjemaer for kvalitetsoppfølging, avvikshåndtering, endringshåndtering og sikkerhetsregler er basis for at banken kan oppnå ønsket kvalitet på IT-tjenestene. Forankring av prosessene i banken og oppfølging av at rutinene blir

fulgt og brukt, er like viktig for å nå kvalitetsmålene. Banken har derfor definert etterlevelse av internt regelverk som et eget kvalitetsmål.

Oppfølging av kvalitetsmålene og rapportering
Basis for oppfølging av hvordan kvalitetsmålene er nådd, er faste månedlige rapporter fra ComputerAssistent og SpareBankKompaniet og bankens egen avvikslogg for hendelser, problemer og feilsituasjoner (se kap. 5).

IT-leder skal hver måned levere en rapport (Kvalitetsrapporten) til ledelsen i banken hvor tall fra følgende kvantitative målinger skal inngå:

- Rapport fra ComputerAssistent som viser tilgjengelighet til systemene og prosentvis oppfyllelse i forhold til avtalte krav

- Rapport fra SpareBankKompaniet som viser tilgjengelighet til systemer som i systemrangeringen er kategorisert til kritisk grad 1 og 2 som driftes av andre enn ComputerAssistent

- Rapport som viser antall registrert henvendelser og definerte problemsituasjoner i avviksloggen

Kvalitetsrapporten skal også inneholde:

- Angivelse av siste måneds aktivitet i forhold til sikkerhetsreglene på IT-siden (nye ansatte, oppdateringskurs for ansatte, endringer / oppdateringer i sikkerhetsreglene)

- Kort status fra IT-leder over hva som har vært de største utfordringene på IT-siden i inneværende periode og hva som antas å bli de største utfordringene i kommende periode (neste måned).

Rapporten behandles på det månedlige møtet mellom IT-leder og bankens ledelse. IT-driftsansvarlig deltar i møtet etter behov. Kvalitetsrapporten skal foreligge hos bankens ledelse minimum tre arbeidsdager før møtet.

Kapittel 4: Sikkerhet

Ref. IKT-forskriftens § 5 Sikkerhet

> ***§ 5 Sikkerhet***
>
> *Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare. Oppfyllelse av kravene til informasjonssikkerhet for personopplysninger etter forskrift av 15 12.2000 nr 1265 til personopplysningsloven skal anses som oppfyllelse av kravene i paragrafen her.*

Hvordan sikre kundene i BankBukkeneBruse IT-tjenester med høy sikkerhet?
Til tross for at BankBukkeneBruse har utkontraktert vesentlige deler av IT-virksomheten, er banken ansvarlig hvis en av bankens kunder får sin konto kompromittert eller data om bankens kunder kommer på avveie. BankBukkeneBruse ser med bekymring på den siste tidens uheldige utvikling hva gjelder kompromittering av nettbank og vil være en pådriver for at sikkerhetsaspektet står i fokus.

I brukerforumet for banker i SpareBankKompaniet er sikkerhetsaspektet høyt på dagsorden og sikkerhetsaspektet har blitt stadig sterkere vektlagt ved revisjonene av avtalen med SpareBankKompaniet. Fra medio 2004 inngår det i avtalen med SpareBankKompaniet at bankene skal motta halvårlige rapporter om status på sikkerhetsarbeidet i SpareBankKompaniet. Videre har SpareBankKompaniet forpliktet seg overfor bankene i sammenslutningen, om å vektlegge sikkerhetsaspektet ved alle anbudsforespørsler til leverandører om IT-produkter og - tjenester. SpareBankKompaniet skal på vegne av sparebankene i gruppen, delta i felles sikkerhetsfora som arrangeres i regi av bankforeningene og Kredittilsynet. Informasjon fra disse møteplassene skal inngå som del av den halvårlige rapporteringen fra SpareBankKompaniet til bankene.

Administrasjon av tilgangskontroller
BankBukkeneBruse er en mindre sparebank med få ansatte og begrenset IT-virksomhet i eget hus, men opererer et stort spekter av IT-systemer. Banken har derfor lagt vekt på å lage et ryddig system for administrasjon av tilgangsrettigheter. Tilgangsrettighetene er basert på prinsippene

- *need to know*
- *least privileges*
- *segregation of duties*

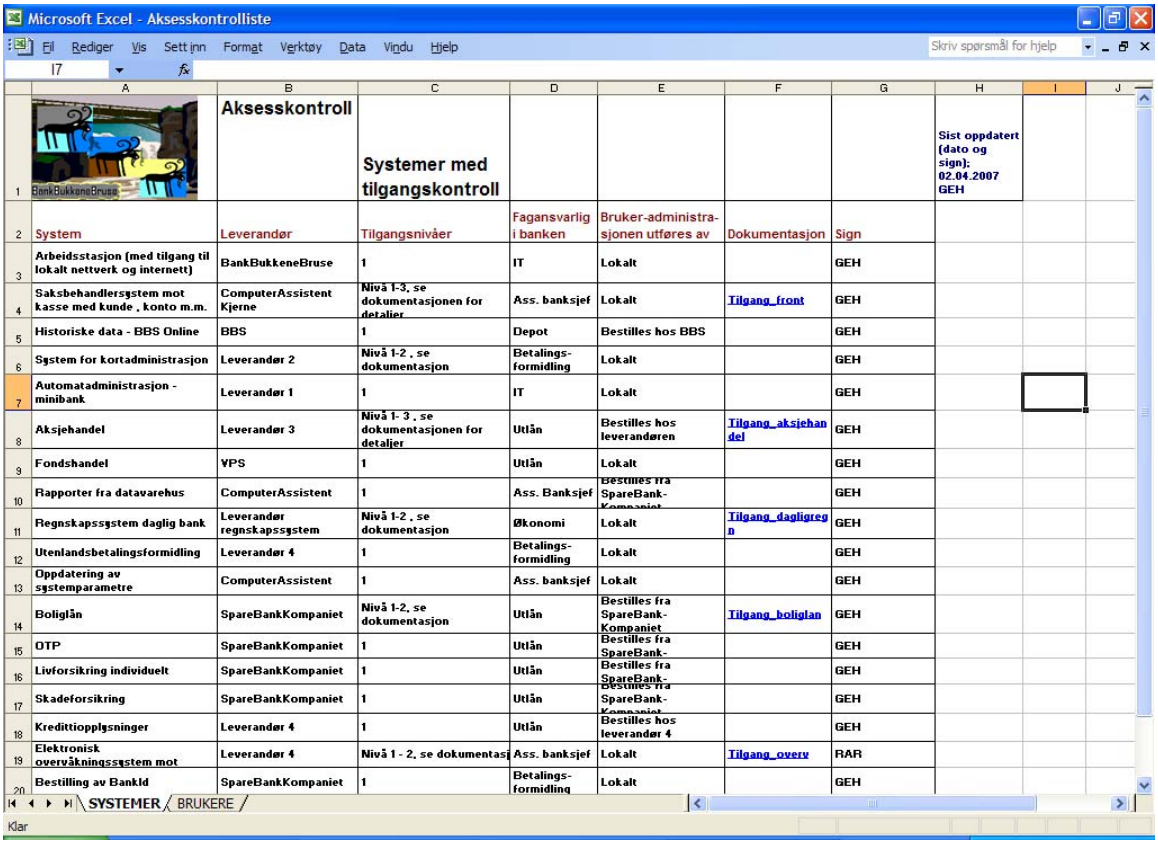
Fagavdelingene har ansvar for å tildele tilgangsrettigheter mens IT-sikkerhetsansvarlig har ansvar for å oppdatere systemene og dokumentasjonen. Når ansatte begynner, endrer arbeidsoppgaver eller slutter i banken, fyller ansvarlig for fagavdelingen ut et skjema som angir hvilke systemer den ansatte skal ha tillagt tilgang til eller fjernet tilgang fra. Skjemaet underskrives av ansvarlig for fagavdelingen og leveres IT-sikkerhetsansvarlig

som har ansvar for å oppdatere tilgangskontrolldokumentasjonen og påføre dato for når tilgangsrettigheter til brukeren er lagt inn i systemet.

En del av systemene har flere nivåer av tilgangsrettigheter. Hvilke rettigheter de ulike nivåene representerer, er beskrevet i systemdokumentasjonene det er lenke til i skjemaet. Nivåene er hierarkisk inndelt slik at en bruker som er tildelt høyeste rettighetsnivå automatisk har tilgang til funksjoner i nivåene under.

Månedlige stikkprøver
IT-leder gjør en månedlig stikkprøvekontroll på at tilgangsrettigheter er korrekt oppdatert. Det kvitteres ut i tilgangskontrolldokumentasjonen av stikkprøvekontroll er gjennomført.

Her er et utsnitt fra administrasjonssystemet for tilgangsrettigheter:



Microsoft Excel - Aksesskontrolliste

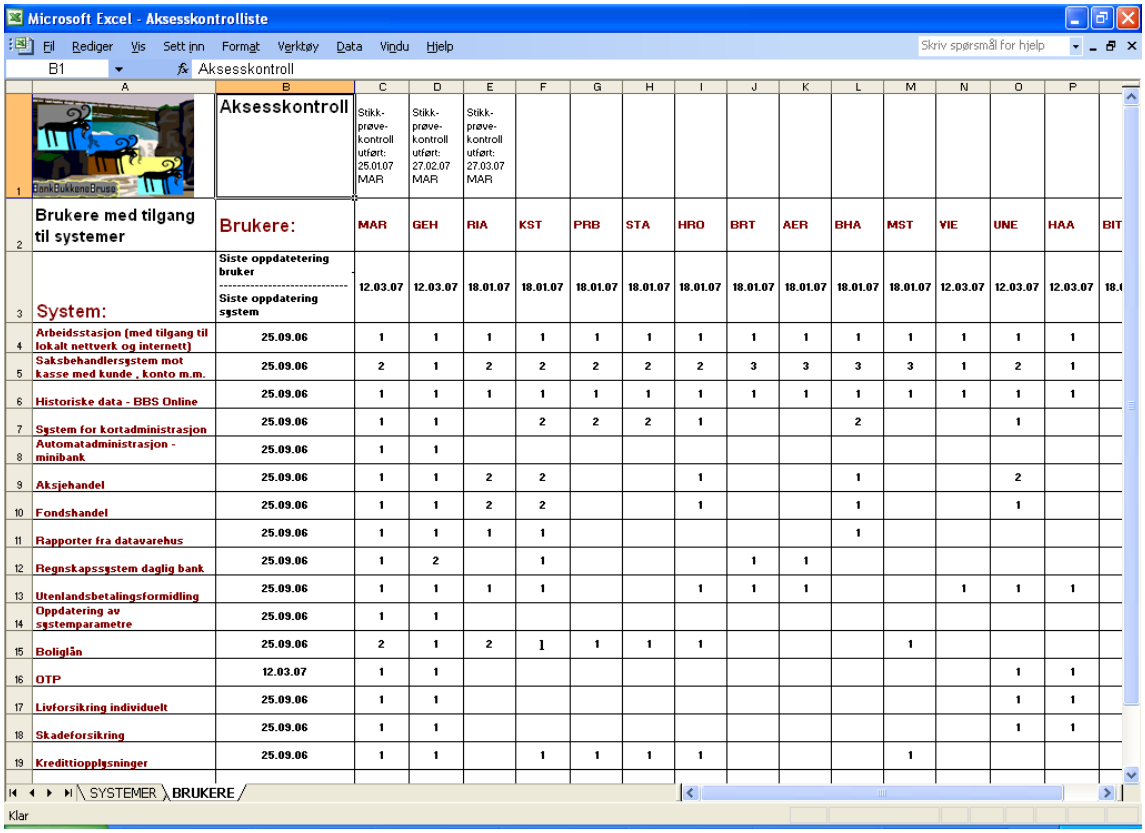
Fil Rediger Vis Sett inn Format Verktøy Data Vindu Hjelp — Skriv spørsmål for hjelp

I7

	A	B	C	D	E	F	G	H	I	J
1	BankBukkeneBruse	**Aksesskontroll**	**Systemer med tilgangskontroll**					Sist oppdatert (dato og sign): 02.04.2007 GEH		
2	System	Leverandør	Tilgangsnivåer	Fagansvarlig i banken	Bruker-administra-sjonen utføres av	Dokumentasjon	Sign			
3	Arbeidsstasjon (med tilgang til lokalt nettverk og internett)	BankBukkeneBruse	1	IT	Lokalt		GEH			
4	Saksbehandlersystem mot kasse med kunde , konto m.m.	ComputerAssistent Kjerne	Nivå 1-3, se dokumentasjonen for detaljer	Ass. banksjef	Lokalt	Tilgang_front	GEH			
5	Historiske data - BBS Online	BBS	1	Depot	Bestilles hos BBS		GEH			
6	System for kortadministrasjon	Leverandør 2	Nivå 1-2 , se dokumentasjon	Betalings-formidling	Lokalt		GEH			
7	Automatadministrasjon - minibank	Leverandør 1	1	IT	Lokalt		GEH			
8	Aksjehandel	Leverandør 3	Nivå 1- 3 , se dokumentasjonen for detaljer	Utlån	Bestilles hos leverandøren	Tilgang_aksjehandel	GEH			
9	Fondshandel	VPS	1	Utlån	Lokalt		GEH			
10	Rapporter fra datavarehus	ComputerAssistent	1	Ass. Banksjef	Bestilles fra SpareBank-Kompaniet		GEH			
11	Regnskapssystem daglig bank	Leverandør regnskapssystem	Nivå 1-2 , se dokumentasjon	Økonomi	Lokalt	Tilgang_dagligregn	GEH			
12	Utenlandsbetalingsformidling	Leverandør 4	1	Betalings-formidling	Lokalt		GEH			
13	Oppdatering av systemparametre	ComputerAssistent	1	Ass. banksjef	Lokalt		GEH			
14	Boliglån	SpareBankKompaniet	Nivå 1-2, se dokumentasjon	Utlån	Bestilles fra SpareBank-Kompaniet	Tilgang_boliglan	GEH			
15	OTP	SpareBankKompaniet	1	Utlån	Bestilles fra SpareBank-Kompaniet		GEH			
16	Livforsikring individuelt	SpareBankKompaniet	1	Utlån	Bestilles fra SpareBank-Kompaniet		GEH			
17	Skadeforsikring	SpareBankKompaniet	1	Utlån	Bestilles fra SpareBank-Kompaniet		GEH			
18	Kredittopplysninger	Leverandør 4	1	Utlån	Bestilles hos leverandør 4		GEH			
19	Elektronisk overvåkningssystem mot	Leverandør 4	Nivå 1 - 2, se dokumentasj	Ass. banksjef	Lokalt	Tilgang_overv	RAR			
20	Bestilling av BankId	SpareBankKompaniet	1	Betalings-formidling	Lokalt		GEH			

SYSTEMER / BRUKERE

Klar



Microsoft Excel - Aksesskontrolliste

Fil Rediger Vis Sett inn Format Verktøy Data Vindu Hjelp — Skriv spørsmål for hjelp

B1 — Aksesskontroll

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
1	BankBukkeneBruse	**Aksesskontroll**	Stikk-prøve-kontroll utført: 25.01.07 MAR	Stikk-prøve-kontroll utført: 27.02.07 MAR	Stikk-prøve-kontroll utført: 27.03.07 MAR												
2	**Brukere med tilgang til systemer**	**Brukere:**	MAR	GEH	RIA	KST	PRB	STA	HRO	BRT	AER	BHA	MST	VIE	UNE	HAA	BIT
3	System:	Siste oppdatetering bruker / Siste oppdatering system	12.03.07	12.03.07	18.01.07	18.01.07	18.01.07	18.01.07	18.01.07	18.01.07	18.01.07	18.01.07	18.01.07	12.03.07	12.03.07	12.03.07	18.(
4	Arbeidsstasjon (med tilgang til lokalt nettverk og internett)	25.09.06	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
5	Saksbehandlersystem mot kasse med kunde , konto m.m.	25.09.06	2	1	2	2	2	2	2	3	3	3	3	1	2	1	
6	Historiske data - BBS Online	25.09.06	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
7	System for kortadministrasjon	25.09.06	1	1		2	2	2	1			2			1		
8	Automatadministrasjon - minibank	25.09.06	1	1													
9	Aksjehandel	25.09.06	1	1	2	2			1			1			2		
10	Fondshandel	25.09.06	1	1	2	2			1			1			1		
11	Rapporter fra datavarehus	25.09.06	1	1	1	1						1					
12	Regnskapssystem daglig bank	25.09.06	1	2		1				1	1						
13	Utenlandsbetalingsformidling	25.09.06	1	1	1	1			1	1	1			1	1	1	
14	Oppdatering av systemparametre	25.09.06	1	1													
15	Boliglån	25.09.06	2	1	2	1	1	1	1				1				
16	OTP	12.03.07	1	1											1	1	
17	Livforsikring individuelt	25.09.06	1	1											1	1	
18	Skadeforsikring	25.09.06	1	1											1	1	
19	Kredittopplysninger	25.09.06	1	1		1	1	1	1				1				

SYSTEMER / BRUKERE

Klar

Retningslinjer for IT-sikkerhet i BankBukkeneBruse
Bankene har utarbeidet en to-delt instruks for intern IT-sikkerhet. Den ene delen inneholder sikkerhetsregler IT-organisasjonen i banken har ansvar for å implementere og etterleve. Den andre delen inneholder sikkerhetsregler alle ansatte i banken er ansvarlige for å etterleve. Nedenfor er det listet opp hovedpunktene i retningslinjene.

IT-sikkerhetsinstruks: Del en: ansvar: IT-organisasjonen:

- Installasjon og vedlikehold av antivirusprogramvare
- Installasjon og vedlikehold av perimeterbeskyttelse (brannmur m.m.)
- Patching av operativsystem
- Rutiner for backup av filserver og server for programvare
- Regler for passordgenerering og – bytte
- Prosedyre ved mistanke om vellykket virusangrep på PC:

  - *Bruker melder fra til IT-drift@BankBukkeneBruse.no*
  - *Infisert maskin fjernes fra nettverket*
  - *Situasjonen kartlegges, er flere maskiner infisert?*
  - *Infisert PC undersøkes for identifikasjon av hva slags virus det er*
  - *Hva kan smittekilden være?*
  - *Antivirusprogramvare med signatur for aktuelt virus installeres*
  - *Infiserte maskiner renses*

IT-sikkerhetsinstruks: Del to: ansvar: alle ansatte i banken:

- Regler for bruk av PC på kontoret
- Regler for bruk av bærbar PC hjemme eller på reise

Forankring av IT-sikkerhetsreglene i banken
IT-sikkerhetsansvarlig er ansvarlig for å implementere, vedlikeholde og drifte oppgavene som er beskrevet i del en av IT-sikkerhetsinstruksen. Dette utgjør en vesentlig del av IT-driftsansvarliges oppgaver.

Del to av sikkerhetsreglene som gjelder for alle ansatte i banken, blir årlig revidert av IT-sikkerhetsansvarlig. Alle nyansatte skal som en del av introduksjonen for nyansatte, innkalles til et møte med IT-sikkerhetsansvarlig for en gjennomgang av reglene. Banken har vurdert sikkerhetsaspektet som så viktig at dette skal være et fast tema på bankens årlige seminar for alle ansatte. IT-sikkerhetsansvarlig er der tildelt en halv time til gjennomgang av IT-sikkerhetsreglene med vekt på eventuelle endringer fra forrige år.

Kapittel 5: Avvikshåndtering

Ref. IKT-forskriftens § 9. Avviks- og endringshåndtering

> ***§ 9 Avviks- og endringshåndtering***
>
> *Foretaket skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges.*
>
> *Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand i IKT-virksomheten. Avviksbehandlingen skal identifisere årsaken til avvik, hindre gjentagelser og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres. Prosedyrene for avvikshåndtering skal inneholde retningslinjer for eskalering.*
>
> *Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.*

Sparebanken BankBukkeneBruse har vurdert ITIL-prosessene Incident Management og Problem Management. IT-organisasjonen er for liten til å implementere dette som to separate prosesser. Banken har isteden valgt å bruke elementer fra begge disse inn i en felles prosess: Avvikshåndtering

Sparebanken BankBukkeneBruse har etablert et felles mottak for henvendelser til brukerstøtte og et felles system for registrering og oppfølging av avvik, problemer og feil med IT-systemene, avviksloggen.

Henvendelser til brukerstøtte kan være

- Rapportering av hendelser eller oppfølging av tidligere rapporterte hendelser fra ComputerAssistent
- Rapportering av hendelser eller oppfølging av tidligere rapporterte hendelser fra SpareBankKompaniet
- Rapportering av feil eller problemer fra bankens ansatte eller direkte fra kunder

Avvik, problemer og feil skal rapporteres enten pr. telefon til brukerstøtte eller til e-postadressen IT-drift@bankbukkenebruse.no. IT-driftsansvarlig har hovedansvar for å betjene telefoner og e-post til brukerstøtte. IT-leder fungerer som stedfortreder til denne tjenesten. I perioder hvor banken har IT pliktkandidat (jamfør kap. 1), kan IT-leder delegere deler av brukerstøtteoppfølgingen til pliktkandidaten som ledd i kompetansebygging.

En vesentlig del av henvendelsene vil være e-post / telefoner fra SpareBankKompaniets felles brukerstøtteapparat og fra ComputerAssistent's feilrapporteringsdisk. Dette kan være svar på tidligere henvendelser fra banken eller informasjon om problemer som har oppstått. Det inngår i IT-driftsleders ansvar å informere bankens ansatte om kjente feil og problemer som er meldt gjennom leverandørenes brukerstøtteapparat. Ved alvorlige feil i selvbetjeningskanalene skal det legges ut beskjed til kundene på www.BankBukkeneBruse.no. Eksempel på en slik feil er manglende tilgjengelighet til nettbank med varighet utover to timer.

Alle IT-relaterte hendelser skal registreres i Avviksloggen. Henvendelser fra bankens ansatte som gjelder rutineforespørsler om tilgang til systemer, utstyr eller programvare er unntatt fra dette.

Avviksloggen gir plass til følgende informasjon om hendelsen:

- Dato for når hendelsen skjedde
- Tidspunkt for når hendelsen skjedde
- Kilde
- Saksbehandler fra kilden
- System
- Beskrivelse av hendelsen
- Saksbehandler i banken
- Alvorlighetsgrad
- Beskrivelse av løsning
- Kobling til andre poster i Avviksloggen
- Status
- Dato for når feilen er løst
- Tidspunkt for når feilen er løst

Avviksloggen skal alltid fylles ut. Det er lagt vekt på å forenkle utfyllingen mest mulig. Noen felt har predefinerte alternative verdier. Alle felt behøver ikke fylles ut. Avviksloggen er laget i excel slik at banken kan benytte sorterings- og statistikkmulighetene i dette verktøyet til å ta ut ulike statistikker over avvik. Hendelsesbeskrivelsen skrives / limes rett inn i rapporten eller det legges inn en lenke til et dokument med beskrivelsen, det samme gjelder løsningsbeskrivelsen.

Disse feltene har predefinerte verdier:

<u>Kilde:</u>
SBK (SpareBankKompaniet)
CA (ComputerAssistent)
Lokal (bruker eller kunde)

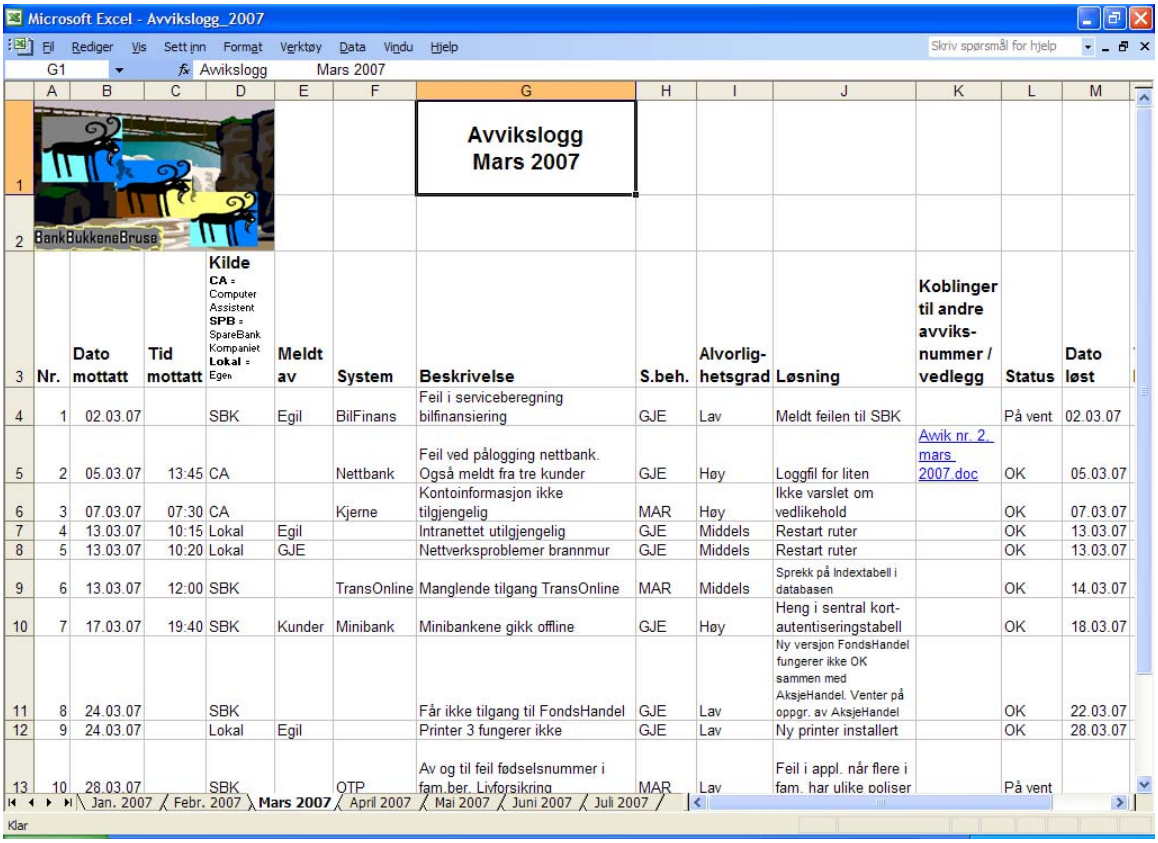
<u>Alvorlighetsgrad:</u>
Høy
Middels
Lav

<u>Status:</u>
Blankt (mottatt)
Avventer
OK

IT-driftsansvarlig kategoriserer alvorlighetsgraden til hendelen til lav, middels eller høy.

Sparebanken BankBukkeneBruse bruker Avviksloggen som et verktøy til å måle kvaliteten. Avviksloggen er en av kildene til den månedlige kvalitetsrapporteringen og kvalitetsoppfølgingen.

Her er Avviksloggen for mars 2007:



Microsoft Excel - Avvikslogg_2007

Fil Rediger Vis Sett inn Format Verktøy Data Vindu Hjelp — Skriv spørsmål for hjelp

G1 — Avvikslogg Mars 2007

Avvikslogg Mars 2007

BankBukkeneBruse

Nr.	Dato mottatt	Tid mottatt	Kilde (CA = Computer Assistent, SPB = SpareBank Kompaniet, Lokal = Egen)	Meldt av	System	Beskrivelse	S.beh.	Alvorlighetsgrad	Løsning	Koblinger til andre avviksnummer / vedlegg	Status	Dato løst
1	02.03.07		SBK	Egil	BilFinans	Feil i serviceberegning bilfinansiering	GJE	Lav	Meldt feilen til SBK		På vent	02.03.07
2	05.03.07	13:45	CA		Nettbank	Feil ved pålogging nettbank. Også meldt fra tre kunder	GJE	Høy	Loggfil for liten	Awik nr. 2. mars 2007.doc	OK	05.03.07
3	07.03.07	07:30	CA		Kjerne	Kontoinformasjon ikke tilgjengelig	MAR	Høy	Ikke varslet om vedlikehold		OK	07.03.07
4	13.03.07	10:15	Lokal	Egil		Intranettet utilgjengelig	GJE	Middels	Restart ruter		OK	13.03.07
5	13.03.07	10:20	Lokal	GJE		Nettverksproblemer brannmur	GJE	Middels	Restart ruter		OK	13.03.07
6	13.03.07	12:00	SBK		TransOnline	Manglende tilgang TransOnline	MAR	Middels	Sprekk på Indextabell i databasen		OK	14.03.07
7	17.03.07	19:40	SBK	Kunder	Minibank	Minibankene gikk offline	GJE	Høy	Heng i sentral kort-autentiseringstabell		OK	18.03.07
8	24.03.07		SBK			Får ikke tilgang til FondsHandel	GJE	Lav	Ny versjon FondsHandel fungerer ikke OK sammen med AksjeHandel. Venter på oppgr. av AksjeHandel		OK	22.03.07
9	24.03.07		Lokal	Egil		Printer 3 fungerer ikke	GJE	Lav	Ny printer installert		OK	28.03.07
10	28.03.07		SBK		OTP	Av og til feil fødselsnummer i fam.ber. Livforsikring	MAR	Lav	Feil i appl. når flere i fam. har ulike poliser		På vent	

Jan. 2007 | Febr. 2007 | **Mars 2007** | April 2007 | Mai 2007 | Juni 2007 | Juli 2007

Klar

Kapittel 6: Endringshåndtering, anskaffelse og installasjon
Ref. IKT-forskriftens §§ 6 Utvikling og anskaffelse og 9 Avviks- og endringshåndtering

§ 6 Utvikling og anskaffelse

Foretaket skal ha skriftlige prosedyrer for anskaffelse, utvikling, videreutvikling og testing av IKT-systemer. IKT-systemene skal ikke settes i ordinær drift før ansvarlig har godkjent dette.

§ 9 Avviks- og endringshåndtering

Foretaket skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges.

Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand i IKT-virksomheten. Avviksbehandlingen skal identifisere årsaken til avvik, hindre gjentagelser og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres. Prosedyrene for avvikshåndtering skal inneholde retningslinjer for eskalering.

Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

Anskaffelse
IT-avdelingen i BankBukkeneBruse har ansvar for innkjøp av maskinvare og programvare for installasjon på lokale arbeidsstasjoner i banken. Dette innebærer også ansvar for håndtering av lisensavtaler og avtaler om automatiske oppdateringer av operativsystem og basis programvare.

BankBukkeneBruse utvikler ikke egen programvare. Sentrale forretningsapplikasjoner knyttet til bankens kjernevirksomhet leveres av ComputerAssistent. Øvrige forretningsapplikasjoner velges fra SpareBankKompaniets applikasjonsportefølje. Beslutning om reduksjon eller økning i bankens systembaserte tjenesteportefølje blir tatt av bankens ledelse.

Inventarlista
Sparebanken BankBukkeneBruse har laget en inventarliste som inneholder informasjon om utstyr knyttet til IT-virksomheten. Lista er delt i tre slik:
- maskinvare installert lokalt i banken eller i filialen
- programvare installert lokalt inkludert lisensavtaler
- programvare fra leverandør

For hvert objekt i lista skal disse opplysningene registreres:
- navn på maskin- /programvare
- status for om maskin- /programvaren er i bruk eller er utrangert,
- versjonsnummer på maskin- /programvare som er i bruk
- leverandør av maskin- /programvare
- dato for siste oppgradering
- signaturen til den som har kvittert ut godkjente testresultater og som har godkjent installasjonen

- dato for når lisensavtale er inngått
- dato for når lisensavtale utgår
- evt. lenke til lisensavtale

IT-driftsansvarlig er ansvarlig for å oppdatere de to første delene av inventarlista; lokalt installert maskinvare og lokalt installert og lisensiert programvare. IT-leder er ansvarlig for å oppdatere den siste delen; programvare fra leverandør.

Endringshåndtering
Sparebanken BankBukkeneBruse definerer endringer og endringshåndtering i IKT-virksomheten som
a) å ta i bruk ny maskinvare, lisensiert programvare eller programvare fra leverandør
b) håndtere nye versjoner eller feilrettinger av maskinvare, lisensiert programvare eller programvare fra leverandør

Banken kan initiere og medvirke til endringer i applikasjoner og i applikasjonsutvalg gjennom brukerforum, men det normale er at banken blir informert om endringer i og nye versjoner av programvare gjennom SpareBankKompaniet eller gjennom ComputerAssistent. Endringer i konfigurasjon eller drift av lokal maskinvare eller programvare initieres derimot direkte gjennom banken. Likeledes oppgraderinger av kontorstøtteprodukter og lokalt installerte sikkerhetsprodukter.

Test
Før banken tar i bruk ny maskin eller programvare eller nye versjoner av eksisterende maskin eller programvare, skal systemene som berøres av endringene, testes.
Hver forretningsapplikasjon skal ha egen testperm hvor testprosedyren for applikasjonen er beskrevet samt at det skal være vedlegg for dokumentasjon av gjennomførte tester. IT-avdelingen har ansvar for å opprette og vedlikeholde testpermer for alle forretningsapplikasjoner. Normalt vil leverandør av applikasjonen levere input til testprosedyren. Test gjennomføres oftest av IT-driftsleder eller IT-leder, men kan i enkelte tilfeller delegeres til andre ansatte i banken. Resultatet av testen skal signeres av den som har utført testen. I tillegg skal alltid IT-leder kvittere ut godkjent testresultat med en egen signatur. Dersom testresultatet ikke er tilfredsstillende slik at testen ikke kan godkjennes og applikasjonen ikke kan installeres, er det IT-leders ansvar å kommunisere og følge opp feilrapportene med leverandøren.

Mindre endringer i systemparametere eller konfigurasjonsoppsett som ikke relaterer seg direkte til en forretningsapplikasjon, skal kvitteres ut som godkjent i Endringsloggen (se under).

Dokumentasjon gjennom Endringsloggen
Av flere årsaker vurderer Sparebanken BankBukkeneBruse det som viktig å kjenne til alle endringer som skal skje og som har skjedd i IT-systemene. For det første er dette viktig for å kunne informere og forberede brukere og kunder om endringer som kommer. Dernest er kjennskap til endringer som har skjedd, en uvurderlig kilde til oppklaring av uønskede hendelser som oppstår i IT-virksomheten. Banken har derfor vedtatt å gi høy

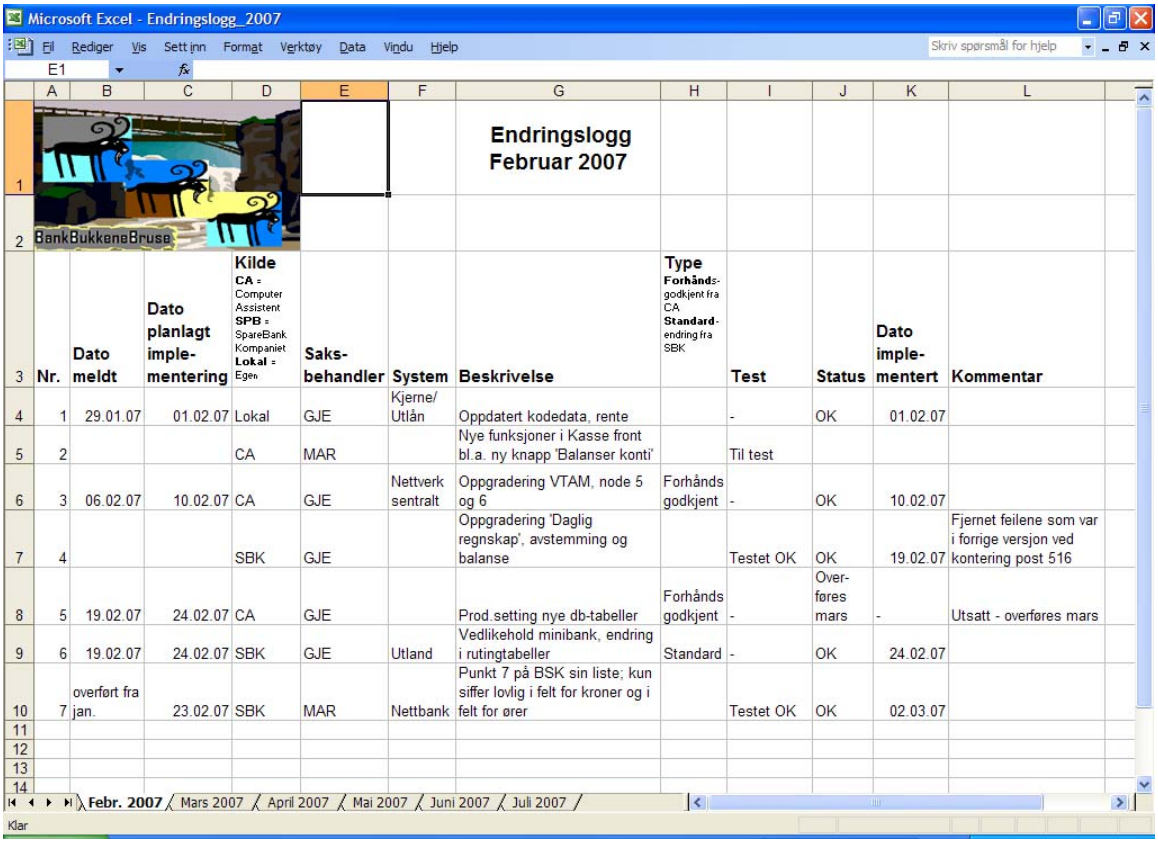
prioritet til at alle endringer skal registreres i Endringsloggen (se mer om denne under). Dette gjelder også endringer leverandørene har definert som forhåndsgodkjente eller standard endringer.

Forhåndgodkjente /standard endringer
ComputerAssistent har definert en gruppe endringer som forhåndsgodkjente. Dette gjelder i stor grad konfigurasjonsendringer på basis programvare på sentrale maskiner som for eksempel oppdateringer på disker, nettverk eller database. SpareBankKompaniet har definert en del applikasjonsendringer som standardendringer. Dette gjelder mindre oppdateringer på en gruppe definerte systemer. Banken har gjennom avtalen med SpareBankKompaniet sikret at alle endringstyper som defineres som forhåndsgodkjente av ComputerAssistent og endringstyper som defineres som standard endringer fra SpareBankKompaniet, årlig dokumenteres skriftlig for banken. Banken har videre gjennom avtalen med SpareBankKompaniet, sikret at banken informeres når det skjer denne typen endringer på systemene. I praksis skjer dette ved at banken hver fredag mottar en oversikt over forhåndsgodkjente / standard endringer som ble implementert inneværende uke samt forhåndsgodkjente / standard endringer som er planlagt implementert kommende uke. Banken tester ikke disse endringene, men de skal registreres i endringsloggen. Det er IT-leders ansvar å oppdatere endringsloggen, og i dette inngår det å avstemme oversikten over inneværende ukes implementerte endringer med forrige ukes planlagte endringer. Dersom det avdekkes større avvik, kan dette være et tema på det månedlige møtet med SpareBankKompaniet.

Opplæring
Når nye IT-baserte tjenester tas i bruk eller ved endringer i eksisterende systemer, skal IT-leder tilrettelegge for nødvendig opplæring. IT-leder kan delegere selve opplæringen til andre ansatte i banken.

Sjekkpunkt dokumentasjon av implementerte endringer:
Er inventarlista oppdatert?
Er endringsloggen oppdatert?

Slik så Endringsloggen for februar 2007 ut:



Microsoft Excel - Endringslogg_2007

Fil Rediger Vis Sett inn Format Verktøy Data Vindu Hjelp — Skriv spørsmål for hjelp

E1

Endringslogg Februar 2007

BankBukkeneBruse

Nr.	Dato meldt	Dato planlagt imple-mentering	Kilde **CA** = Computer Assistent **SPB** = SpareBank Kompaniet **Lokal** = Egen	Saks-behandler	System	Beskrivelse	Type **Forhånds**-godkjent fra CA **Standard**-endring fra SBK	Test	Status	Dato imple-mentert	Kommentar
1	29.01.07	01.02.07	Lokal	GJE	Kjerne/ Utlån	Oppdatert kodedata, rente		-	OK	01.02.07	
2			CA	MAR		Nye funksjoner i Kasse front bl.a. ny knapp 'Balanser konti'		Til test			
3	06.02.07	10.02.07	CA	GJE	Nettverk sentralt	Oppgradering VTAM, node 5 og 6	Forhånds godkjent	-	OK	10.02.07	
4			SBK	GJE		Oppgradering 'Daglig regnskap', avstemming og balanse		Testet OK	OK	19.02.07	Fjernet feilene som var i forrige versjon ved kontering post 516
5	19.02.07	24.02.07	CA	GJE		Prod.setting nye db-tabeller	Forhånds godkjent	-	Over-føres mars	-	Utsatt - overføres mars
6	19.02.07	24.02.07	SBK	GJE	Utland	Vedlikehold minibank, endring i rutingtabeller	Standard	-	OK	24.02.07	
7	overført fra jan.	23.02.07	SBK	MAR	Nettbank	Punkt 7 på BSK sin liste; kun siffer lovlig i felt for kroner og i felt for ører		Testet OK	OK	02.03.07	

Ark: Febr. 2007 | Mars 2007 | April 2007 | Mai 2007 | Juni 2007 | Juli 2007

Klar

Kapittel 7: Kontinuitet

Ref. IKT-forskriftens §§ 7 Systemvedlikehold, 8 Drift og 10 Krav til kontinuitet

§ 7 Systemvedlikehold

Foretaket skal sikre at IKT-systemene vedlikeholdes og forvaltes på en måte som gir en stabil, planlagt og forutsigbar drift. Det skal foreligge dokumenterte prosedyrer for systemvedlikeholdet.

§ 8 Drift

Driften av IKT-virksomheten skal være basert på dokumenterte prosedyrer, som sikrer fullstendig, rettidig og korrekt dataproduksjon, behandling og oppbevaring av produksjonsdata samt tilgjengelighet av IKT-systemene.

§ 10 Krav til kontinuitet

Foretaket skal ha en oppdatert kontinuitetsplan. Foretaket skal etablere en prosedyre for kontinuitet hvor roller, ansvarsoppgaver og risiko defineres. Foretaket skal med bakgrunn i risikoanalyse, jf. § 3, definere IKT-systemer av betydning for foretakets virksomhet som skal dekkes av kontinuitetsplanen. Kontinuitetsplanen skal blant annet inneholde

-identifisering og vurdering av enkeltelementer som kan svikte og iverksette tiltak
-klare kriterier for oppstart av reserveløsningen
-gjenopprettingsprosedyrer
-informasjon til ledelse, ansatte, eventuelt kunder og leverandører.

Det skal gjennomføres opplæring, øvelse og testing av reserveløsningene i et omfang som gir trygghet for at reserveløsningene fungerer tilfredsstillende. Testene skal dokumenteres slik at gjennomføring og resultat kan vurderes i ettertid.

BankBukkeneBruse har veldefinerte prosedyrer for drift og vedlikehold av IT-virksomheten inkludert et sett med sikkerhetsregler, og vurderer dette som ledd i å sikre kontinuitet i de IT-baserte tjenestene. Beskrivelse av driftsrutiner og nødvendig informasjon er samlet i egen perm og lagret elektronisk på Driftsoppfølging og avbruddshåndtering.

Lokal drift og systemvedlikehold som utføres av egen IT-organisasjon i banken
IT-driftsansvarlig har ansvar for at følgende driftsoppgaver blir utført:

- Daglig backup av filer på filserver og server for programvare. Backup tas til egen backupserver og i tillegg til medium for ekstern lagring. Detaljert beskrivelse av backuprutinene finnes i eget kapittel i permen Driftsoppfølging og avbruddshåndtering.
- Daglig kontroll av virusdeteksjon
- Daglig kontroll av perimeterbeskyttelse
- Ukentlig vedlikeholdskontroll av tekniske komponenter; modem, switcher, routere, huber, skrivere, scanner

Frafall eller feil i komponenter banken håndterer
Avbrudd kan ha ulike årsaker. I en del tilfeller er årsaken til avbruddet feil i systemer eller systemkomponenter som banken selv drifter pga strømbrudd, kommunikasjonsbrudd mot dataleverandør som følge av feil i teleleverandørs linjer/nett, feil på modem, routere, switcher eller huber. For å minimalisere konsekvensen ved bortfall eller feil på noen av

disse komponentene, har banken UPS-aggregat, dupliserte linjer og et lager av nettverkskomponenter som kan installeres på kort varsel.

I en krisesituasjon kan en minimumsløsning etableres gjennom bruk av de bærbare PC'ene.

Feil i sentrale systemer
For de sentrale systemene er BankBukkeneBruse prisgitt leverandørenes drifts- og kontinuitetsløsninger. Avbrudd i sentrale systemer skal rapporteres uten ugrunnet opphold av leverandøren til bankens brukerstøtte. Banken behandler avvikene i henhold til bankens avvikshåndteringsprosess med dokumentasjon i avviksloggen. Avvikene blir videre fulgt opp gjennom kvalitetsrapporteringen. Gjennom SLA-avtalene er en tilgjengelighetsgaranti for hvert system definert. Målt tilgjengelighet til hvert system samt avvik fra garantert tilgjengelighet, er en del av den månedlige rapporteringen fra leverandøren. SLA avtalene inneholder sanksjoner ved brudd mot avtalte servicenivåer.

Kapittel 8: Katastrofeberedskap

Ref. IKT-forskriftens § 11 Driftsavbrudd og katastrofeberedskap

§ 11 Driftsavbrudd og katastrofeberedskap

Foretaket skal ha en dokumentert katastrofeplan som skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en katastrofe. Med katastrofe menes hendelser som forårsaker driftsavbrudd slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser.

Katastrofeplanen skal minst omfatte

-oversikt over IKT-systemer som inngår i katastrofeplanen
-beskrivelse av katastrofeløsningen
-klare kriterier for oppstart av katastrofeløsningen
-akseptabel lengde på et driftsavbrudd før katastrofeløsningen iverksettes
-prosedyrer som inneholder de nødvendige aktiviteter for å gjenopprette IKT-driften
-oversikt over ansvarsforhold og prosedyrer ved oppstart av katastrofeløsningen
-informasjon til berørte ansatte, leverandører, kunder, offentlige myndigheter og media.
Det skal minst en gang årlig gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt. Resultatet av testen skal dokumenteres slik at det er mulig å kontrollere.

BankBukkeneBruse har etablert en katastrofeberedskap. Denne er beskrevet i bankens Katastrofeplan. Katastrofeplanen er et eget dokument og ikke en del av denne håndboka. Her i håndboka redegjør vi for hovedelementene i planen.

Oppbevaring og oppdatering av katastrofeplanen
Katastrofeplanen omfatter bankens samlede katastrofeberedskap og er ikke begrenset til IT-virksomheten. I en krisesituasjon er det av vesentlig betydning av katastrofeplanen er oppdatert og tilgjengelig. Katastrofeplanen oppbevares i papirformat og på CD med et eksemplar i banken og et eksemplar i filialen. I tillegg er Katastrofeplan tilgjengelig fra bankens intranettsider. Bankens ledelse har delegert oppgaven med å oppdatere katastrofeplanen til IT-leder. I tillegg til å oppdatere planen med endringer som påvirker innholdet i planen, skal planen rutinemessig revideres hver 6. måned. Katastrofeplanen har versjonshåndtering slik at det til enhver tid fremgår når planen sist ble oppdatert eller revidert. Sammen med katastrofeplanen oppbevares en katastrofepakke, se nærmere om denne under.

Beredskapsorganisasjon og ansvar for å erklære en katastrofesituasjon
Katastrofeplanen beskriver beredskapsorganisasjonen som består av bankens ledelse, IT-leder og ytterligere to av bankens ansatte. Det er bankens ledelse som erklærer en katastrofesituasjon.

Kontakt internt og eksternt i en krisesituasjon
Planen inneholder varslingslister med telefonnummer, epost-adresser og adresser til alle i beredskapsorganisasjonen. Videre inneholder den kontaktinformasjon (firma og kontaktpersoner) til aktuelle IT-leverandører og leverandører av annen infrastruktur til banken. Katastrofeplanen beskriver regler for kommunikasjonsveier internt i banken og

med leverandørene i en krisesituasjon. Den beskriver også retningslinjer for informasjon til kundene og til pressen.

Papirbaserte reserveløsninger
Banken har utarbeidet et opplegg for papirbaserte reserveløsninger for inn- og utbetalinger og mottak av betalingsoppdrag i en overgangsperiode til IT-baserte løsninger er reetablert.

Katastrofeplanen er videre delt i to hoveddeler;
LokalPlanKatastrofe og SystemSviktKatastrofe.

LokalPlanKatastrofe skal dekke den situasjonen at bankens virksomhet er satt ut av spill grunnet problemer knyttet til bankens lokaler eller utstyr. Dette kan være brann, strømbrudd, brudd på telenettet, vannlekkasje, eksplosjon, epidemi eller andre situasjoner som gjør at bankens virksomhet ikke kan fortsette med normalt tilgjengelige ressurser. Bankens tjenester gjennom selvbetjeningskanalene vil fungere. Planen beskriver etablering av bankens hovedfunksjoner på alternativt driftsted i filialens lokaler i nabobygda. Det er satt opp en prioriteringsrekkefølge på funksjoner ved reetablering:

- Kasse/ ekspedisjon / sentralbordfunksjon
- Økonomi / likviditet
- Betalingsformidling
- Utlån
- Depot
- Andre funksjoner

Sammen med katastrofeplanen oppbevares en katastrofepakke bestående av:

- Grovskisse nettverk
- Kodedata
- Originalsoftware
- Backup
- Skjematur til å håndtere papirbasert drift
- Dokumentasjon

IT-leder har ansvar for å oppdatere katastrofepakken. På samme måte som med selve katastrofeplanen skal dokumentene i pakken oppdateres ved endringer som påvirker innholdet og i tillegg rutinemessig revideres hver 6. måned og revideringen kvitteres ut at er gjennomført:

Dato	Katastrofeplan oppdatert / revidert	Kommentar	Katastrofepakke Oppdatert / revidert	Kommentar	Signatur
10.03.07	OK		OK	Lagt til nye konfigurasjonsparametre	MAR
14.09.07	OK	Oppdatert	OK	MS VISTA	MAR

		kontaktinfo varslingslister			

Test og øvelse LokalPlanKatastrofe

Banken bruker IKT-forskriftens krav om at det "*en gang årlig gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt* " som rettesnor i forhold til test av lokal katastrofeplan. Bankens ledelse har laget en plan for testing og et opplegg for å gjennomføre test. Resultatet av testene dokumenteres i permen: TestLokalPlanKatastrofe

Svikt i tilgjengelighet til sentrale systemer.
Den andre hoveddelen av bankens katastrofeplan har fått navnet SystemSviktKatastrofe. Denne behandler en situasjon der bankens lokaler er intakte, men bankens IT-systemer ikke er tilgjengelige grunnet problemer utenfor bankens egen rekkevidde. Banken har laget en prioriteringsrekkefølge på systemene, se Systemrangeringen i kap. 2.

I avtalen med SpareBankKompaniet er katastrofeløsning for bankens sentrale IT-systemer beskrevet. Dette omfatter i første rekke systemene med basis i bankens kjerneløsning i ComputerAssistent. På vegne av bankene i sammenslutningen har SpareBankKompaniet inngått avtale om en felles katastrofeløsning for bankene som benytter denne kjerneløsningen. Gjennom avtalen er det sikret at leverandøren oppfyller kravet om at kjerneløsningen er duplisert på alternativt driftssted i tilstrekkelig lang geografisk avstand fra utgangspunktet. Bankens selvbetjeningskanal med tilgang til nettbank, er etter systemrangeringen gjennomført våren 2006, rangert som bankens mest kritiske applikasjon. BankBukkeneBruse har sammen med andre banker gjennom brukerforumet presset på for at tilstrekkelige reserveløsninger for nettbank skal etableres. Fra våren 2007 har BankBukkeneBruse fått avtalefestet at nettbankløsningen kan reetableres på alternativt plattform i en krisesituasjon. I avtalene er beskrevet kriterium for oppstart av katastrofeløsningene.

Test og øvelse SystemSviktKatastrofe.
I avtalen med SpareBankKompaniet er opplegget for test og øvelse i katastrofeplanene beskrevet. SpareBankKompaniet distribuerer en halvårlig testplan hver 6. måned. Ca hver 3. måned deltar banken i test eller mottar resultater av tester gjennomført sentralt. IT-leder er ansvarlig for å lagre dokumentasjon av disse testene i permen TestSystemSviktKatastrofe.

Kapittel 9: Dokumentasjon

Ref. IKT-forskriftens § 13 Dokumentasjon

§ 13 Dokumentasjon
Det skal foreligge en samlet oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet og som dokumenterer at forskriftens krav er oppfylt til enhver tid.

BankBukkeneBruse har dokumentert IT-virksomheten gjennom følgende avtaler, planverk og dokumentasjon:

- Håndbok for IKT-virksomheten i BankBukkeneBruse (dette dokumentet)
- Avtale med SpareBankKompaniet
- Systemrangering
- Risikoanalyse
- Administrasjonssystem for tilgangsrettigheter
- IT-sikkerhetsinstruks
- Avvikslogg
- Inventarliste
- Endringslogg
- Testpermer
- BackupPerm
- Katastrofeplan
- Nettverkskonfigurasjon
- Kodedata