

AAU Use cases

Indhold

AAU Use cases	1
Applikation til ITSM	3
Arbejdskalender	4
Backup	6
Bruger ikke i AD	7
Brugergrænseflader.....	8
Change	10
Cyberangreb	12
Dashboards.....	13
Dataudveksling i formular og proces gennem systemintegration	14
Etablering af integration.....	16
Events	17
Grafisk systemoverblik i CMDB	19
Håndtering af fortrolig sag	20
Incident.....	21
Indsamling/discovery af CMDB data	23
Knowledge artikler – intern og ekstern	24
Konfigurering af CI-relationer i CMDB.....	25
Logning	26
Mailskabelon	27
Major Incident	29
Oprettelse af trigger	31
Opsætning og konfigurering af CMDB.....	32
Problem	34
Rapportering.....	36
Service information	37
Service Level Agreement	38
Service Request	39
Sikkerhedshændelse – bortkommen enhed	41
Styring af udlån.....	42

Ændringer til dokumentet

Dato	Beskrivelse	Udført af
20-12-2022	Dokument oprettet	HHL

Om dokumentet

Dokumentet indeholder use cases der beskriver arbejdsgange på Aalborg Universitet. Use casene skal benyttes til at demonstrere og vurdere, hvordan de enkelte ITSM-systemer håndterer de forskellige situationer.

ITSM-systemernes funktionalitet vil blive vurderet ud fra hvordan godt de enkelte use cases løses, og i hvor høj grad løsningen kræver special konfiguration.

Use casene er listet i alfabetisk orden, og rækkefølgen er ikke et udtryk for prioriteten.

Applikation til ITSM

Use Case	
Navn	Applikation til ITSM
Formål	ITSM skal kunne benyttes på alle mobile enheder via en applikation.
Begyndelsesbetingelse	Oprettelse af sag via applikation
Slutbetingelse	Afslutning af sag via applikation
Forventet aktører	Bruger, Support Level 1
Forretningsregler	
Scenarie	Peter opretter en sag via ITSM applikation. Support Level 1 løser og lukker Peters henvendelse i ITSM Peter får via applikationen en notifikation om, at hans henvendelse er blevet løst og lukket.
Opgave	Vis og forklar, hvordan applikation kan bruges til oprettelse og håndtering af sager.

Arbejdskalender

Use Case	
Navn	Arbejdskalender
Formål	Oprettelse af arbejdskalender til brug ved beregning af brud på SLA
Begyndelsesbetingelse	Vi nærmer os et nyt år
Slutbetingelse	Arbejdskalender er klar
Forventet aktører	Systemadministrator
Forretningsregler	Udover almindelige helligdage, har AAU en række dage der er tvungne fridage
Scenarie	Det er sidst på året, så der skal oprettes en arbejdskalender for 2023. Systemadministrator logger på systemet og går i gang med at definere arbejdsdage for 2023. Der registreres forskellige dagstyper, fx: Hverdag SupportHverdag SupportTorsdag Fredag Weekend Helligdag Halv helligdag AAU dag Der defineres åbningstider for hver dagtype. Når det er gjort, oprettes 2 kalendere. En for Support og en for alle andre. Alle dage i kalenderåret, registreres med en af ovenstående dagstyper. Systemadministrator opretter en sag, for at se om arbejdskalenderen anvendes korrekt i forhold til SLA: 1) Beregnes tiden korrekt i sagen i forhold til arbejdskalenderen? 2) Sendes der besked, når Påbegynd tidspunkt overskrides? 3) Vises det i sagsoversigten at SLA er brudt? 4) Sendes der besked, når Løst tidspunkt overskrides? 5) Kan der skelnes i sagsoversigt om SLA er brud på Påbegyndt eller Løst tidspunkt? 6) Systemadministratoren sætter sagen i Vent. 7) Genberegnes tiden korrekt i forhold til SLA og Ventetype?
Opgave	Vi og forklar hvordan ITSM understøtter Use Casen med særlig fokus på: ○ Oprettelse af kalender og dagstyper ○ Hvordan forskellige grupper er tilknyttet forskellige kalendere ○ Hvordan kalender bruges til at beregne urgencies fra en SLA. ○ Hvordan urgency genberegnes når en sag sættes i Vent. ○ Hvordan der skelnes mellem venttyper

Backup

Use Case	
Navn	Backup
Formål	At demonstrere Leverandørens tilbud om backup af data i Systemet.
Begyndelsesbetingelse	Der sker et driftsnedbrud af Systemet med tab af noget af Kundens data.
Slutbetingelse	Systemets drift er reetableret med den nyeste backup af Systemets data.
Forventet aktører	Leverandøren
Forretningsregler	
Scenarie	1. Der sker et driftsnedbrud af Systemet med tab af nogle af Kundens data. 2. Leverandøren informerer uden unødvendig forsinkelse Kunden om driftsnedbruddet. 3. Leverandøren reetablerer Systemets drift med den nyeste backup af Systemets data. Leverandøren informerer løbende Kunden om status på reetableringen.
Opgave	1. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvordan Leverandøren sikrer backup af Systemets data. ○ Hvordan data i backup beskyttes på mindst samme sikkerhedsniveau, som data i Systemet. ○ Hvordan data i backup sikres mod ransomware. ○ Hvordan Systemet kan gendannes ved alle former for nedbrud. - Herunder ▪ hvordan Systemets kan gendannes ved nedbrud, der ikke involverer tab af Kundens data i Systemet, uden at gendannelsen medfører tab eller ændring af Kundens data. ▪ hvordan Systemets kan gendannes ved nedbrud, der involverer tab af Kundens data, på baggrund af sidste backup af Systemets data. ○ Hvordan persondata for enkeltpersoner kan slettes og/eller anonymiseres i backup for overholdelse af GDPR.

Bruger ikke i AD

Use Case	
Navn	Bruger ikke i AD
Formål	Det skal være muligt for brugere uden en aau konto, f.eks. kommende studerende, at oprette sager via serviceportalen.
Begyndelsesbetingelse	Ny studerende har spørgsmål vedr. kommende studieplads.
Slutbetingelse	Behandling af henvendelse fra eksterne (bruger uden aau konto) er foregået fra start til slut via ITSM
Forventet aktører	Bruger Support Level 1
Forretningsregler	AAU håndterer alle henvendelser, det være sig blandt andet ansatte, konsulenter, gæster og kommende studerende.
Scenarie	Rikke skal starte på nyt studie pr 1. februar og har i den forbindelse diverse spørgsmål. Rikke tilgår serviceportalen, hvor hun stiller de spørgsmål hun måtte have. Support Level 1, modtager henvendelsen Support Level 1 besvarer Rikke og lukker sagen Rikke får besked via serviceportalen og personlig mail, at der er kommet svar på hendes spørgsmål
Opgave	Vis og forklar, hvordan denne Use Case understøttes, med særlig fokus på: ○ Hvordan ITSM understøtter at alle henvendelser fra serviceportalen oprettes som sager, også selvom vedkommende ikke har en aau konto (bruger ikke oprettet i AD) ○ Hvordan oplysninger om brugeren registreres i ITSM ○ Hvordan bruger bliver underrettet via personlig mail, ved svar på henvendelsen.

Brugergrænseflader

Use Case	
Navn	Brugergrænseflader
Formål	At demonstrere Systemets brugergrænseflader.
Begyndelsesbetingelse	En Bruger skal oprette en Service Request.
Slutbetingelse	En Sagsbehandler er i gang med at sagsbehandle Service Requesten.
Forventet aktører	Bruger, Support Level 1, Support Level 2, Sagsbehandler.
Forretningsregler	
Scenarie	4. En Bruger tilgår Systemets brugergrænseflade og opretter en Service Request. 5. En sagsbehandler åbner sit personlige dashboard i Systemet og ser Service Requesten. 6. Sagsbehandleren begynder sagsbehandlingen af Service Requesten, og erfarer, at der er behov for, at Brugeren uploader noget dokumentation. Sagsbehandleren skriver dette til Brugeren gennem Systemet. 7. Brugeren modtager en notifikation om, at der er nyt i sagen. 8. Brugeren tilgår Systemets brugergrænseflade, og ser at han/hun skal uploade noget dokumentation. Brugeren uploader den efterspurgte dokumentation. 9. Sagsbehandleren ser på sit dashbord, at der er nyt på sagen. 10. Sagsbehandleren forsætter sagsbehandlingen af sagen.
Opgave	2. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvordan Systemet understøtter et transparent serviceforløb for Brugere, dvs. at Brugere præsenteres for et tydeligt, visuelt overblik over, hvor i serviceworkflowet vedkommende befinder sig, og hvad der forventes af vedkommende på hvilke tidspunkter. ○ Hvordan det fremgår tydeligt af Systemets brugergrænseflade, fx ved brug af farver eller ikoner, både hvilke handlinger Brugeren skal udføre lige nu, men også hvilke handlinger der allerede er fuldførte, og hvilke Brugeren kan forventes at skulle udføre i fremtiden. ○ Hvordan dashboards kan opsættes individuelt, så den enkelte sagsbehandler får det ønskede overblik. F.eks. grupperinger af sager efter kategori, Sagsansvarlig, prioritering o.l. ○ Hvordan en sagsbehandler selv kan bestemme både rækkefølgen af kolonner og hvilke kolonner der vises på vedkommendes dashboard. ○ Hvordan der er mulighed for individuel tilpasning af felter på dashboards, samt mulighed for at kunne sortere på disse felter. ○ Hvordan det er muligt for sagsbehandlere at oprette, gemme og genbruge søgninger. Både til individuelt genbrug og til fælles

	genbrug, hvor en søgning kan genbruges af flere sagsbehandlere. Fx hvis en sagsbehandler opretter en søgning, der finder alle incidents, som vedrører MFA problemer, indenfor den sidste uge, hvorefter vedkomne gemmer søgningen og deler den med andre sagsbehandlere, som derefter kan genbruge søgningen. ○ Hvordan en sagsbehandler gennem Systemets brugergrænseflade kan se historik på en sag, der viser alt, hvad der er udført på sagen. Alle hændelser skal være logget og kunne ses. Der skal være timestamp, før og efterværdi samt aktør på alle hændelser. ○ Hvordan det er muligt at navigere i Systemets brugergrænseflade via genvejstaster (uden brug af mus). ○ Hvordan det er tænkt ind i Systemets brugergrænseflade, at brugere kan navigere i Systemet med få klik. ○ Hvordan brugere og specialister kan bruge tabulatorer til at navigere i brugergrænsefladen. ○ At Systemets brugergrænseflade ikke har små klikbare felter, som kan være svære at ramme.
--	--

Change

Use Case	
Navn	Change
Formål	ITSM-håndtering af en change
Begyndelsesbetingelse	Ændringsønsker og/eller fejlmeldinger
Slutbetingelse	
Forventet aktører	Support Level 1, Support Level 2, Support Level 3, Configuration Manager, Change Manager
Forretningsregler	
Scenarie	- Support Level 1 modtager en del servicerequests på ændringsønsker til IdM IT-servicen. - Support Level 1 registrerer disse servicerequests med kategoriseringskode RFC e.l. De tilknyttes IT-servicen IDM og SLA'en for ændringsønsker tilknyttes. Impact sættes til middel, da det kun er administratorer i IdM der er berørte. Prioriteten sættes ud fra reaktionstiden på SLA'en og Impact. Sagen tildeles IDM gruppen (Support Level 2) som sagsansvarlig. Support Level 1 forbliver Koordinator af sagen. - IDM-gruppen opretter en normal change ud fra en foruddefineret IDM-change template. - Change template indeholder en spørgeguide, der er relevant for denne type change. - Change template indeholder et aktivitets flow, der er relevant for denne type change. - IdM-gruppen udpeger en changeansvarlig, som analyserer og planlægger change. - Den changeansvarlige skal sikre, at de nødvendige ressourcer – både mennesker og teknik er til stede til at udføre change. - Den changeansvarlige planlægger de enkelte aktiviteter i changeflowet, og tildeler de enkelte aktiviteter til de relevante personer. De enkelte aktiviteter planlægges med start og slut tidspunkter, der tager hensyn til dels hvornår der er ressourcer tilgængelige og dels at de enkelte aktiviteter udføres i den rigtige rækkefølge. Det er vigtigt, at der indhentes accept af ressourcer. - Den changeansvarlige vurderer sammen med specialisterne om der er behov for hjælp fra Support Level 3, og indhenter accept af dette, samt tilpasser aktivitetsworkflowet.

	10. En aktivitet i changeflowet frigives automatisk, når den foregående aktivitet er afsluttet, og den aktivitsansvarlige får en notifikation om at aktiviteten er frigivet. 11. Når planlægning er klar, starter udvikling. Samtidig med udvikling påbegyndes udarbejdelse af dokumentation og testcases. 12. Når de 3 aktiviteter alle er afsluttet, skal der gennemføres en acceptancetest. 13. Hvis testen accepteres, frigives CAB-aktiviteten, og changen skal godkendes af Change Advisory Board (CAB). Når CAB-aktiviteten frigives, skal det fremgå i changekalenderen, at den er klar til vurdering i CAB. 14. Hvis testen ikke accepteres, resettes alle aktiviteter, og changen returnerer til planlægningsaktiviteten. Den changeansvarlige orienteres om dette, og planlægning af change begynder forfra. 15. Godkendes changen af CAB, skal brugerne i god tid orienteres om, at IdM opdateres. Orienteringen skal indeholde beskrivelse af ændringerne. Support Level 1 skal også orienteres. 16. På implementeringsdagen notificeres brugerne om, at IdM er utilgængelig, og så kan implementeringen begynde. 17. Databasefolkene tilføjer eventuelle ændringer til databasen, og derefter deployes softwareændringer af IdM-gruppen og databasefolkene. 18. IdM-gruppen opdaterer Git. 19. CMDB skal opdateres med nyt Git#. Det er Configuration Manager der er ansvarlig for, at CMDB'en bliver opdateret. 20. Herefter meldes der ud om, at IdM igen er kørende. 21. Reviewaktiviteten frigives, når alle implementeringsaktiviteter er lukkede. Den changeansvarlige review'er evt. sammen med changemanager opgaveforløbet, og vurderer om der er noget i processen, der skal ændres. 22. Changen lukkes, og alle de tilknyttede sager går i status løst. 23. Herefter kan Support Level 1 lukke sagerne.
Opgave	Vis og gennemgå ovenstående flow. Fokus skal primært være på at vise flow mellem aktiviteterne og de forskellige aktører.

Cyberangreb

Use Case	
Navn	Cyberangreb
Formål	At demonstrere Leverandørens beredskab og beredskabsplan for håndtering af cyberangreb.
Begyndelsesbetingelse	Leverandøren udsættes for et hackerangreb.
Slutbetingelse	Hackerangrebet er afværget og Systemets drift er normal.
Forventet aktører	Leverandøren
Forretningsregler	
Scenarie	11. Leverandøren udsættes for et hackerangreb. 12. Leverandøren aktiverer Leverandørens beredskab og beredskabsplan for håndtering af cyberangreb. Herunder informerer Leverandøren Kunden uden unødvendig forsinkelse om Systemets drift status. 13. Leverandøren holder løbende Kunden orienteret om status. 14. Leverandøren afværger hackerangrebet og sikrer, at Systemets drift er normal.
Opgave	3. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Leverandørens Beredskab og beredskabsplan.

Dashboards

Use Case	
Navn	Dashboards
Formål	At demonstrere, hvordan systemet understøtter opsætning af individuelle brugergrænseflader/overblik via dashboards for Specialister, som giver samlede, relevante overblik over sager og deres status, herunder: - at indhold i den individuelle brugergrænseflade opdateres i realtid. - at den individuelle brugergrænseflade giver Specialisten overblik over sager indenfor vedkommendes arbejdsområde. - at det er tydeligt for Specialisten, hvis der er sager, som kræver handling af vedkommende. - at det er tydeligt for Specialisten, hvis der er sket ændringer til sager. - at Specialisten kan tilføje relevante søge- og filtreringsparametre til sin individuelle brugergrænseflade. - at Specialisten med få klik og i samme arbejdsgang kan bevæge sig mellem den individuelle brugergrænseflade og den detaljerede sagsbehandling.
Begyndelsesbetingelse	
Slutbetingelse	
Forventet aktører	Support Level 1, Support Level 2
Forretningsregler	
Scenarie	
Opgave	Vis hvordan man på baggrund af alle tilgængelige data i ITSM laver individuelle dashboards.

Dataudveksling i formular og proces gennem systemintegration

Use Case	
Navn	Dataudveksling i formular og proces gennem systemintegration
Formål	At demonstrere at felter i en online formular automatisk udfyldes med information, der hentes gennem en integration mellem Systemet og et andet af Kundens systemer, og at Systemet overfører information til et andet af Kundens systemer.
Begyndelsesbetingelse	Den studerende Bent ønsker at oprette en sag via Self Service Portalen, da han har tabt sit adgangskort til Kundens lokaler.
Slutbetingelse	Sag oprettet i Service Desk
Forventet aktører	Rekvirent
Forretningsregler	
Scenarie	15. Bent ønsker at oprette en sag via Self Service Portalen, da han har mistet sig adgangskort til Kundens lokaler. 16. Bent logger in på Self Service Portalen gennem Kundens autentifikationsløsning (i dag Azure Active Directory). 17. Systemet får information om Bents navn, e-mail adresse hos Kunden og studienummer fra Kundens autentifikationsløsning. 18. Self Service Portalen viser en formular til sagsoprettelse. 19. Bent vælger via en drop down på formularen, at hans problem vedrører hans adgangskort. 20. Systemet henter information om Bents nuværende adgangskort gennem en integration mellem Systemet og Kundens system til styring af adgangskort. 21. Systemet udfylder automatisk felter med information om Bents adgangskort på formularen (fx kort nummeret) og viser en ny drop down, hvor Bent kan vælge, hvilken service han ønsker i forbindelse med hans adgangskort. 22. Bent vælger via drop down "Jeg har tabt mit adgangskort, og jeg ønsker et nyt adgangskort". 23. Bent trykker på "Opret sag" og sagen oprettes i Systemet med relevant kategorisering på fx CI. 24. Bent modtager en kvitteringsmail om oprettelsen af hans sag. 25. Systemet sender informationen om, at Bents har tabt sit adgangskort, samt at Bent ønsker et nyt adgangskort til Kundens system til styring af

	adgangskort gennem en integration mellem Systemet og Kundens system til styring af adgangskort. 26. Kundens system til styring af adgangskort lukker Bents tabte kort, og igangsætter en proces til produktion af et ny adgangskort til Bent. 27. Kundens system til styring af adgangskort informerer Systemet om forventet leveringstid af Bent nye adgangskort til Systemet. 28. Systemet sender en e-mail til Bent, med informationen om forventet leveringstid af det nye adgangskort. 29. Kundens system til styring af adgangskort informerer Systemet om, at Bents nye adgangskort er klar til afhentning. 30. Systemet sender en e-mail til Bent med informationen om, at det nye adgangskort er klar til afhentning. 31.processens fortsættelse er ikke interessant for denne Use Case....
Opgave	4. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ hvordan Systemet automatisk kan hente data fra et andet system og autoudfylde felter i en formular, som en Rekvirent eller en Sagsbehandler er ved at udfylde. ○ Hvordan Systemet kan overføre data til og hente data fra et andet system som en del af en proces, der er konfigureret i Systemet.

Etablering af integration

Use Case	
Navn	Etablering af integration
Formål	At demonstrere hvordan Kunden egenhændig kan etablere en integration mellem Systemet og et andet af Kundens systemer gennem Systemets API.
Begyndelsesbetingelse	Kunden ønsker at etablere en integration mellem Systemet og et andet af Kundens systemer gennem Systemets API.
Slutbetingelse	Der er etableret en integration mellem Systemet og et andet af Kundens systemer gennem Systemets API.
Forventet aktører	Software udvikler hos Kunden.
Forretningsregler	
Scenarie	32. En software udvikler hos Kunden etablerer en integration mellem Systemet og et andet af Kundens systemer gennem Systemets API. Der udføres Create, Read, Update og Delete operationer gennem integrationen.
Opgave	5. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvilke services og operationer (herunder Create, Read, Update og Delete) Systemet tilbyder gennem Systemets API. ○ Hvordan Systemets API understøtter en hændelsesorienteret arkitektur (Event Driven Architecture). ○ Sikkerhed i forbindelse med integrationer mellem Systemet og et andet af Kundens systemer gennem Systemets API, herunder Systemets understøttelse af forskellige sikkerhedsmekanismer i forbindelse med integration gennem Systemets API. ○ Fejlfinding i forbindelse med integrationer mellem Systemet og et andet af Kundens systemer gennem Systemets API. ○ Logning i forbindelse med integrationer mellem Systemet og et andet af Kundens systemer gennem Systemets API. ○ Begrænsninger i forbindelse med integrationer mellem Systemet og et andet af Kundens systemer gennem Systemets API.

Events

Use Case	
Navn	Events
Formål	At demonstrere hvordan Systemet kan interagere med Kundens overvågningssystemer.
Begyndelsesbetingelse	Kundens overvågningssystem Microsoft System Center Operations Manager (SCOM) detekterer en netværksfejl.
Slutbetingelse	Der er automatisk oprettet en sag af typen Event i Systemet, og Systemet har sendt en status tilbage til SCOM.
Forventet aktør	Sagsbehandler
Forretningsregler	
Scenarie	33. Kundens overvågningssystem Microsoft System Center Operations Manager (SCOM) detekterer en netværksfejl. 34. SCOM sender gennem en integration til Systemet information om netværksfejlen til Systemet. 35. Systemet opretter automatisk en sag af typen Event med høj prioritet med den information typen kræver. 36. Sagen autodispatches til rette sagsbehandler udfra CI'en, der repræsenterer det fejllamte netværk. 37. En Sagsbehandler begynder at behandle af sagen. 38. Systemet sender en status om, at fejlen er under behandling til SCOM. 39. Flere applikationer, som bruger det fejllamte netværk, melder gentagne gange fejl til SCOM. 40. Samtidig melder flere Azure applikationer, som bruger det fejllamte netværk, gentagne gange fejl til Azure Monitor. 41. Både SCOM og Azure monitor sender fejlene til Systemet, gennem deres integration til Systemet. 42. Systemet kan på en intelligent måde koble applikationsfejlene til sagen om netværksfejlen. 43. Systemet sikrer på intelligent vis, at der ikke oprettes dubletter af sager i Systemet, både som følge af at én applikation gentagne gange melder samme fejl, og som følge af at flere applikationer sender fejl ind, som skyldes samme grundlæggende fejl (netværket). Det skal dog være muligt at se, hvor mange fejl der meldes ind. 44. Når der sker statusskifte på sagen i Systemet, sender Systemet den opdaterede status til både SCOM og Azure Monitor.

Opgave	6. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvilke muligheder der er for at integrere Systemet med overvågningssystemer, herunder både API baseret integration og e-mail baseret integration. ○ Hvordan Systemet kan sende status og statusskift på sagsbehandlingen af en fejl, som er meldt ind fra et overvågningssystem til Systemet, til overvågningssystemet. ○ Hvordan Systemet på intelligent vis sikrer, at der ikke oprettes dubletter af sager i Systemet, som følge af at én applikation gentagne gange melder samme fejl. ○ Hvordan Systemet på intelligent vis sikrer, at der ikke oprettes dubletter af sager i Systemet, som følge af at flere applikationer sender fejl ind, som skyldes samme grundlæggende fejl (fx en netværksfejl).
--------	--

Grafisk systemoverblik i CMDB

Use Case	
Navn	Grafisk systemoverblik i CMDB
Formål	At demonstrere hvordan Systemet kan give Kundens Sagsbehandlere og Systemadministratorer et klart og informativt grafisk overblik over CI's og deres sammenhænge i Systemets CMDB, der er relevant for den ITIL-proces overblikket benyttes i.
Begyndelsesbetingelse	Der registreres en sag på en CI der fejler.
Slutbetingelse	Sagsbehandleren har informeret relevante interessenter om konsekvenserne af den fejlende CI. Systemadministrator har igangsat de nødvendige handlinger til genoprettelse af de services, der er ramt af den fejlende CI.
Forventet aktører	Systemadministrator, Sagsbehandler
Forretningsregler	
Scenarie	45. Der registreres en sag på en CI der fejler. 46. En Sagsbehandler åbner sagen, og kan i Systemet se et grafisk overblik, der tydeligt viser de CI's, services og interessenter, der er påvirket af fejlen. 47. Sagsbehandleren sender sagen videre til en relevant Systemadministrator, og informerer relevante interessenter om konsekvenserne af fejlen, og om mulige work arounds. 48. Systemadministrator modtager sagen og åbner et grafisk overblik over CI's, services og anden CMDB data, der har den nødvendige detaljegrad til, at Systemadministratoren kan igangsætte en effektiv og fokuseret analyse, der kan resultere i de nødvendige tiltag til at få de berørte services i drift igen i en rækkefølge, der svarer til deres kritikalitet.
Opgave	7. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ det grafiske overblik over CI's, services og interessenter en Sagsbehandler kan få, når en CI fejler, eller hvis et system kortvarigt skal tages ud af drift pga. nødvendige opgraderinger. Forklar hvordan det grafiske overblik understøtter en effektiv sagsbehandling med det rette informationsniveau til berørte interessenter. ○ det grafiske overblik over CI's, services og anden CMDB data en Systemadministrator kan få, fx hvis en CI fejler, eller hvis et system kortvarigt skal tages ud af drift pga. nødvendige opgraderinger. Forklar hvordan det grafiske overblik understøtter en effektiv og fokuseret analyse, der kan resultere i de nødvendige tiltag til at få de berørte services i drift igen i en rækkefølge, der svarer til deres kritikalitet.

Håndtering af fortrolig sag

Use Case	
Navn	Håndtering af fortrolig sag
Formål	Tilbudsgiver skal vise, hvordan ITSM håndtere fortrolige sager, som kun må være synlig for visse personer. Hvordan disse personer kan se, at sagen er fortrolig og hvordan man kan skjule fortrolige oplysninger, så det er muligt at dele sagen med andre.
Begyndelsesbetingelse	Der modtages en sag med fortrolige oplysninger
Slutbetingelse	Sagen bliver låst for andre sagsbehandlere, som ikke har rettigheder til at tilgå de fortrolige oplysninger. Der kan kommunikeres med sagsbehandlere på tværs, hvor de fortrolige oplysninger bliver skjult
Forventet aktører	Bruger Support Level 1 Support Level 2
Forretningsregler	
Scenarie	Der kommer en henvendelse ind via e-mail, med personfølsomme oplysninger.
Opgave	Vis hvordan en sag kan markeres at den indeholder fortrolige og/eller personfølsomme data. Vis hvordan information i en sag kan markeres som fortrolige og/eller personfølsomme data. Vis hvordan man kan skjule data som ikke skal kunne læses af alle. Vis hvordan data bliver tilgængelige for Support Level 2. Vis hvordan der kan kommunikeres på tværs via sagen, hvor at fortrolige og/eller personfølsomme data kun kan ses af dem som har rettigheder til at se data.

Incident

Use Case	
Navn	Incident
Formål	At følge en sag fra start til slut, med alle handlinger.
Begyndelsesbetingelse	Bruger opretter sag via serviceportalen
Slutbetingelse	Support Level 1 lukker sagen
Forventet aktører	Bruger, Support Level 1
Forretningsregler	Sagen skal altid lukkes af Support Level 1. Sager oprettes primært igennem Service Portal. Brugere må godt henvende sig til Support Level 1 support igennem telefon eller chat.
Scenarie	Sonja ringer til SPOC, da hun ikke kan få sin computer på internettet. Jens fra Support Level 1 opretter en incident, sætter korrekt kategori og prioritering ud fra integreret prioriteringsmatrix. Jens prøver at hjælpe Sonja med at få hendes computer på nettet. Mens sagsbehandling foregår, er sagen låst for at andre kan redigere i sagen. Det er sværere end forventet, så sagen skal videre til Support Level 2. Jens skriver i sagen, hvad han har prøvet. Sagsforløbsentriet logges og kan ikke efterfølgende ændres. Jens glemte en vigtig detalje, så han tilføjer et nyt entry i sagsforløbet. Jens kan ikke huske hvem i Support Level 2 der skal have sagen, så han vælger at tildele sagen til Support Level 2 ud fra den ansvarlige på det tilknyttede CI. Support Level 2 får Sonjas computer på nettet, og skriver i sagens løsningsfelt, hvad der er gjort, og afslutter sagen med korrekte løsningskode. Sonja modtager en mail, med løsningsbeskrivelse og skal bekræfte, at hun er enig i, at sagen er løst. Support Level 1 modtager godkendelse fra Sonja og lukker herefter sagen.
Opgave	Vis og forklar, hvordan usecasen kan håndteres i ITSM. Herunder: ○ Oprettelse af sag ved telefon henvendelse. Søg bruger frem via AD. ○ Sæt korrekt kategori fra integreret liste. ○ Ved løsning af sag, skal der sættes en løsningskategori. Løsningen sendes til bruger. ○ Det skal fremgå af incidenten, at den afventer godkendelse fra bruger. ○ Ved godkendelse skal Support Level 1, modtage en form for notifikation på, at bruger har godkendt løsningen. ○ Sagen lukkes med korrekt lukkekode. Vis og forklar, hvordan man nemt kan danne sig et overblik over sagen.

- | | |
|--|--|
| | <ul style="list-style-type: none">○ Sagsforløb, årsagsbeskrivelse og løsningsbeskrivelse skal stå separat og skal nemt kunne findes frem på sagen. |
|--|--|

Vis, hvordan det kan ses, at sagen er låst for redigering og hvordan man kan se hvem der har låst sagen mod redigering og hvornår sagen blev låst.

Indsamling/discovery af CMDB data

Use Case	
Navn	Indsamling/discovery af CMDB data
Formål	At demonstrere hvordan Kunden effektivt og smidigt kan oprette og ajourføre CMDB data (herunder CI's og deres relationer) i Systemets CMDB gennem automatisk, semi-automatisk og manuel indsamling/discovery fra Kundens it-miljø. Evt. ved brug af hjælpeværktøjer.
Begyndelsesbetingelse	Kunden har konfigureret Systemets CMDB og skal oprette CMDB data. Kunden ønsker, at oprettelse og ajourføring af CMDB data sker så automatisk som muligt.
Slutbetingelse	Dataene i Systemets CMDB afspejler Kundens it-miljø og ajourføres med en høj grad af automatisering.
Forventet aktører	Systemadministrator
Forretningsregler	
Scenarie	49. Systemadministrator Hans konfigurer Systemet og eksterne værktøjer, der automatisk kan indsamle/discover CMDB data (herunder CI's og deres relationer) fra Kundens it-miljø og oprette og ajourføre disse i Systemets CMDB. 50. Systemets CMDB fyldes automatisk med CMDB data (herunder CI's og deres relationer), og disse data ajourføres løbende fremadrettet.
Opgave	8. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ hvordan Systemet og/eller eksterne værktøjer automatisk kan indsamle/discover CMDB data (herunder CI's og deres relationer) fra Kundens it-miljø, og oprette og ajourføre disse i Systemets CMDB. ○ hvordan Systemet kan håndtere, at samme CI indlæses fra forskellige systemer uden at Systemet opretter CI dubletter. ○ Hvordan Systemet reagerer på og adviserer om fejl, der identificeres under den automatiske indlæsning/ajourføring af CMDB data.

Knowledge artikler – intern og ekstern

Use Case	
Navn	Knowledge artikler – intern og ekstern
Formål	At vise hvordan ITSM understøtter knowledge processen. Hvor brugere bliver tilbudt vejledninger eller guides ved oprettelse af sag. At sagsbehandlere bliver tilbudt guides eller workaround til løsning af sag.
Begyndelsesbetingelse	Bruger kan via knowledge artikel selv nå at løse udfordringen, inden sagen når videre til IT.
Slutbetingelse	Bruger og/eller Sagsbehandler har fået den nødvendige viden.
Forventet aktører	Slutbruger Support Level 1
Forretningsregler	
Scenarie	Sonja har fået ny telefon, men hun kan ikke finde ud af at opsætte sin mail på den. Efter opsætning af mail, skal hun også have opsat MFA på sin telefon. 24. Sonja begynder at oprette en sag via Service Portal. Da Sonja begynder at beskrive, hvad hun har brug for hjælp til, får hun tilbudt en top 5 el. top 10 liste over vejledninger der matcher ord, som Sonja bruger i hendes oprettelse. 25. Sonja finder en vejledning til opsætning af mail, som gør Sonja i stand til selv at opsætte mail på telefonen. 26. Derefter har Sonja brug for hjælp til opsætning af MFA på telefonen. Sonja begynder at oprette en sag via Service Portal, og bliver tilbudt relevante vejledninger. Sonja finder en vejledning til opsætning af MFA, men det lykkes hende ikke at få det sat op ved hjælp af vejledningen, hvorfor hun fortsætter sagsoprettelsen. 27. Sagsbehandler begynder at håndtere sagen ved at søge guides frem til opsætning af MFA. 28. Systemet viser de knowledge artikler, der er til opsætning af MFA og sagsbehandler benytter den guide, der er relevant for Sonjas henvendelse. 29. Sagsbehandler løser sagen.
Opgave	1. Vis, hvordan Sonja under sagsoprettelsen i Service Portalen bliver tilbudt vejledninger og guides, der matcher ord i hendes sagsoprettelse. 2. Vis, hvordan Sagsbehandler i Systemet bliver tilbudt vejledninger og guides til at løse sager.

Konfigurering af CI-relationer i CMDB

Use Case	
Navn	Konfigurering af CI-relationer i CMDB
Formål	At demonstrere at opbygning af relationer i Systemets CMDB er fleksibelt, fx ved at fjerne eller tilføje relationer. At demonstrere et grafisk overblik over IT-services og deres sundhedstilstand.
Begyndelsesbetingelse	På foranledning af Systemejer skal der oprettes en ny IT-service med relaterede CIs.
Slutbetingelse	Den nye IT-service kan benyttes i andre processer Det er muligt at synliggøre at fejl på et hvilket som helst CI i IT-servicen, som vil påvirke IT-servicen.
Forventet aktører	Configuration Manager
Forretningsregler	
Scenarie	51. Configuration Manager oprettet et nyt CI af typen "IT-service" 52. Configuration Manager udfylder relevant data, såsom Ansvarlig, Systemejer, Bruger, Lokation, Oppetid, Status m.m. 53. Configuration Manager tilknytter de CIs der indgår i og understøtter IT-servicen. 54. Configuration Manager validerer at IT-servicen er relateret til de rigtige CI i den grafiske visning af IT-servicens CI-hierarki. 55. Configuration Manager validerer at fejl på CIs der indgår i IT-servicen ændrer CIs status, både tekstuelt og visuelt i grafikken.
Opgave	9. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvordan CI-type specifikke felter vises på CI'en ○ hvordan der nemt oprettes relationer mellem CIs ○ hvordan Systemet effektivt og intelligent kan udstiller CI relationer og sundhed grafisk.

Logning

Use Case	
Navn	Logning
Formål	At demonstrere hvordan Systemet understøtter logning af Brugerers og Sagsbehandleres handlinger i Systemet, herunder at Sagsbehandler har adgang til en oversigt over loggede handlinger.
Begyndelsesbetingelse	En Bruger har indsendt en Service Request til Systemet.
Slutbetingelse	Alle logninger kan vises i Systemet.
Forventet aktører	Bruger, Sagsbehandler.
Forretningsregler	
Scenarie	56. En Bruger sender en Service Request til Systemet. Service Requesten indeholder personfølsom information. 57. En Sagsbehandler (Sagsbehandler A) starter behandling af Service Requesten og udfører flere handlinger på sagen. 58. En anden Sagsbehandler (Sagsbehandler B) kommer ved en fejl til at åbne sagen, og ser den personfølsomme information. 59. Systemet logger alle brugerhandling. 60. En Sagsbehandler tilgår Systemets log over Brugerers og Sagsbehandleres handlinger i Systemet, og kan se de handlinger, Brugeren og de to Sagsbehandlere har udført, herunder både at Sagsbehandler A har udført handlinger på sagen, og at Sagsbehandler B har åbnet sagen og set de personfølsomme informationer. 61. Loggen indeholder timestand, aktør, før- og efterværdi og handling.
Opgave	10. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvilke handlinger Systemet kan logge, og fra hvilke aktører. ○ Hvordan det er muligt at konfigurere Systemet til kun at logge specifikke handlinger. ○ Hvordan og hvem der kan tilgå logningsdata i Systemet. ○ Hvordan Systemet logningsdata kan vises, sorteres, filtreres og søges. ○ Hvordan Systemet i nær realtid kan eksportere logningsdata – fx til Kundens centrale logdata system (i dag Splunk).

Mailskabelon

Use Case	
Navn	Mailskabelon
Formål	At vise at der kan oprettes det antal mailskabeloner der er behov for, at der kan defineres logik, så visse kriterier skal være opfyldt før de aktiveres, og at adgang til mailskabeloner kan begrænses
Begyndelsesbetingelse	Risikovurdering af CI er ændret
Slutbetingelse	Relevante brugere er orienteres om ændringen
Forventet aktører	Support Level 1, Support Level 2, Systemadministrator
Forretningsregler	
Scenarie	Scenarie 1) Systemadministrator har oprettet et nyt felt på CI, der viser risikovurderingen for et CI. Der skal nu oprettes en trigger der sender en besked til Systemejer, CI ansvarlig og Support Level 1, når risikovurderingen ændres. Systemadministrator opretter en mailskabelon, som kun er tilgængelig på CIs. Mailskabelonen indeholder oplysninger om: - CI-navn - Systemejer - CI ansvarlig - Ny risikovurdering - Tidligere risikovurdering - Hvem der har foretaget ændringen - Tidsstempel for hvornår ændringen er foretaget. Systemadministrator opretter en trigger, der gør at der sendes en mail baseret på den nyoprettede mailskabelon, når risikovurdering ændres. Scenarie 2) Systemadministratoren opretter en mailskabelon baseret på alle oplysninger på CI, fx: - CI-navn - CI-status - CI ansvarlig - Systemejer - CI bruger - Oppetid - M.m. Mailskabelonen skal benyttes til at sende mail til f.eks. leverandør, Support Level 1, Support Level 2 m.m. Systemadministratoren gør mailskabelonen tilgængelig på CIs, og giver Support Level 2 adgang til at benytte den når de har behovet. Support Level 2 kan sendes mails baseret på mailskabelonen, når de har et CI-billede åbent.

	Support Level 2 skal selv kunne angive modtager af mail, både til/cc/bcc. Og de skal kunne tilføje og fjerne tekst fra mail'en.
Opgave	Vi og forklar hvordan ITSM understøtter Use Casen med særlig fokus på: ○ Oprettelse af Mailskabelon ○ Oprettelse af trigger ○ Begrænsning af tilgængelighed ○ Vælg af mailskabelon ved manuel aktivering.

Major Incident

Use Case	
Navn	Major Incident
Formål	At følge en sag fra start, overgang til major incidentprocessen og til sidst afslutning af major incident.
Begyndelsesbetingelse	En kritisk fejl konstateres.
Slutbetingelse	Sag lukket af Support Level 1
Forventet aktører	Support Level 1 Support Level 2 Major incident manager Taskforce gruppe
Forretningsregler	Al relevant kommunikation og information i forbindelse med Major Incident skal kunne foregå via Systemet.
Scenarie	62. Der kommer mange henvendelser ind fra brugere, som ikke kan tilgå deres filer. 63. Sagsbehandler vurderer sagen til at være en major incident, og kontakter derfor major incident manager. 64. Major incident manager er enig i, at dette skal håndteres som en major incident og indkalder derfor til taskforce møde og opretter Major Incident sag i Systemet. 65. Sagsbehandler laver en serviceinfo og sender en SMS om, at vi nu står med en driftsforstyrrelse, som vi pt ikke kender løsningen på. SMS skal kun udsendes til de brugere, som har tilmeldt sig denne service. 66. Sagsbehandler opdaterer løbende sag, serviceinfo og SMS med fornøden info. 67. Når major incident er løst, sender Systemet opdatering på serviceinfo og SMS. Systemet markerer tilknyttede Incident sager som løst og disse opdateres med samme løsningsbeskrivelse. 68. Sagsbehandler lukker Major Incident efter 5 dag, hvorved Systemet automatisk lukker tilknyttede Incident sager.
Opgave	11. Vis hvordan Sagsbehandler løser sine opgaver i Systemet ○ Oprette Major Incident sag ○ Sende service info – både internt og eksternt ○ Sende SMS 12. Vis hvordan Major Incidents kan gøres synlig for alle interessenter i Systemet.

	13. Vis hvordan Sagsbehandler kan se, når der er nyt i en major incident. 14. Vis hvordan det er nemt for alle sagsbehandlere at følge med i fremdriften på en major incident. 15. Vis hvordan Major Incident sag markeres som løst og efterfølgende lukkes, herunder hvordan tilknyttede Incidents sager derefter automatisk løses og lukkes med samme løsningsbeskrivelse.
--	---

Oprettelse af trigger

Use Case	
Navn	Oprettelse af trigger
Formål	At demonstrere hvordan Kunden selv kan tilføje logik til felter i systemet, der resulterer i en handling. f.eks. ved hjælp af triggere
Begyndelsesbetingelse	Systemadministratoren Mette logger ind i Systemet for at oprette 2 triggere 1) Trigger på Impact i en Incident. 2) Trigger på brugertype på Incident
Slutbetingelse	Logik er tilføjet på feltet Impact.
Forventet aktører	Systemadministrator
Forretningsregler	
Scenarie	69. Mette logger ind i Systemet som systemadministrator. 70. Mette opretter en trigger på feltet Impact. Triggeren aktiveres, når indholdet i feltet opdateres og ved oprettelse af sagen. 71. Triggeren checker på om indholdet ændres til 'Høj'. 72. Der sendes en mail til Major Incident Manager om at der er tale en potentiel Major Incident. 73. Mette validerer at Systemet reagerer på den nye trigger. 74. Mette opretter en trigger på feltet feltet Brugertype. Triggeren aktiveres, når indholdet i feltet opdateres og ved oprettelse af sagen. 75. Triggeren checker på om indholdet ændres til 'SWIP' 76. SLA ændres til SWIP. 77. Mette validerer at Systemet reagerer på den nye trigger.
Opgave	16. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ Hvordan der oprettes speciel logik

Opsætning og konfigurering af CMDB

Use Case	
Navn	Opsætning og konfigurering af CMDB
Formål	At demonstrere opsætning og konfigurering af Systemets CMDB, fx med mulighed for at tilføje custom dataobjekter og felter. At demonstrere at CI's og andet CMDB data kan bruges i andre ITIL processer, fx i sager.
Begyndelsesbetingelse	Systemadministrator Bo logger ind i Systemet for at tilføje custom dataobjekter, relationer og felter til Systemets CMDB.
Slutbetingelse	De ændrede CI's kan benyttes i Incident, Service Request, Problem, Change og Major Incident processerne.
Forventet aktører	Configuration Manager
Forretningsregler	
Scenarie	78. Bo logger ind i Systemet som Systemadministrator. 79. Bo tilføjer custom feltet "Lokation", som angiver hvor CI er placeret fysisk. Bo angiver, at denne oplysning skal hentes fra Kundens Lokations-system. 80. Bo tilføjer Kundens CI typer, CI undertyper og deres hierarki. 81. Bo angiver, hvilke standard og custom felter der er fælles for alle CI's (herunder custom entiteten "Impact") - uanset typen af CI. 82. Bo angiver standard og custom felter for hver CI type og CI undertype, idet felter nedarves i CI type hierarkiet. 83. Bo opdaterer konfigurationen af Incident, Service Request, Problem, Change og Major Incident processerne, således at CI's bruges i sagsbehandlingen. 84. Bo tilføjer og konfigurerer en standard konnektor, der gør, at Systemet kan udveksle CI data med Kundens System Center Configuration Manager (SCCM). 85. Bo validerer at Systemet effektivt og intelligent udveksler CI data med Kundens System Center Configuration Manager (SCCM).
Opgave	17. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ hvordan Systemets CMDB kan konfigureres med CI typer og CI undertyper, og hvordan disse kan opsættes i et CI type hierarki, ○ hvordan felter kan specificeres for CI typer og CI undertyper, der nedarves gennem et CI type hierarki. ○ hvordan custom dataobjekter og custom felter kan tilføjes Systemets CMDB,

	○ hvordan CI's og andet CMDB data (inkl. custom dataobjekter og custom felter) kan tilknyttes og bruges i andre ITIL processer, fx i sager i Incident processen, ○ hvordan Systemet effektivt og intelligent kan udveksle CI data med Kundens System Center Configuration Manager (SCCM) gennem en af Systemets standard konnektorer.
--	---

Problem

Use Case	
Navn	Problem
Formål	At demonstrere registrering og flow i en Problem proces. At demonstrere tydeligt overblik i CI-konfigurationen. At demonstrere registrering og tilgang til Work Around.
Begyndelsesbetingelse	Der meldes pludselig mange fejl ind til Support Level 1.
Slutbetingelse	Problemet er løst, CMDB er opdateret og brugere er informeret.
Forventet aktører	Problem Manager, Support Level 1, Support Level 2
Forretningsregler	
Scenarie	86. Support Level 1 modtager mange henvendelser om at forskellige systemer er utilgængelige. 87. Support Level 1 kontakter Problem Manager med forslag om at oprette en Problem sag. 88. Problem Manager opretter en Problem sag og de indkomne incidents tilknyttes Problem sagen. 89. Problem manager kategoriserer og prioriterer Problem sagen, og der meldes ud på de rette kanaler. 90. Problem Manager afdækker ressourcebehovet, og tildeler Problem sagen til relevant Support Level 2. 91. Support Level 2 indsnævrer "synderen", bl.a. ved hjælp af oversigten over berørte Cis og de relationer disse indgår i. 92. Support Level 2 undersøger, om der er tale om en Known Error. 93. Er det ikke en Known Error, registreres Problem sagen som en Known Error. 94. Support Level 2 går i gang med fejlfinding. 95. Support Level 2 vurderer om fejlen kan omgås. I så fald udarbejdes workaround, som registreres i Knowledge DB, og Support Level 1 orienteres. 96. Herefter går Support Level 2 i gang med at udbedre fejlen. 97. Det konkluderes, at der er behov for en Change, så der oprettes en Change, og Change processen initieres. 98. Når Change er implementeret, lukkes Problem sagen, hvorved de tilknyttede incidents lukkes automatisk.

	99. Known Error og evt. Work Around for Problem sagen arkiveres/gøres ikke aktuel. 100. Der klarmeldes på intern serviceinfo og på serviceportalen.
Opgave	18. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ hvordan CI-relationerne benyttes til at finde den eller de Cis, der fejler, samt hvem der kan hjælpe med udarbejdelse af løsningen, ○ hvordan man holder interessenter orienteret om fremgang ○ hvordan Systemet effektivt og intelligent stiller oplysninger om Known Error og Work Arounds til rådighed. Samt hvordan de registreres.

Rapportering

Use Case	
Navn	Rapportering
Formål	At demonstrere, hvordan der kan laves rapporter, ud fra al data i ITSM
Begyndelsesbetingelse	
Slutbetingelse	
Forventet aktører	
Forretningsregler	
Scenarie	
Opgave	Vis eksempler på nedenstående: Månedlige KPI rapporter der automatisk sendes til bestemte personer: • Hvordan fremfindes data • Hvordan scheduleres rapporten • Hvordan offentliggøres rapporten på portalen • Hvordan tilknyttes rapporten et personligt dashboard Eksport af data til behandling i f.eks. PowerBi • Hvordan laves udtræk Rapport over bestemte sager og deres flow mellem afdelinger Rapport over brudte SLA. Og meget andet

Service information

Use Case	
Navn	Service information
Formål	Deling af driftsinformation med alle brugere
Begyndelsesbetingelse	Driftsforstyrrelse opstår og information skal deles med alle brugere
Slutbetingelse	Brugere er orienteret om driftsstatus
Forventet aktører	Support Level 1
Forretningsregler	
Scenarie	Der opstår nedbrud på print service Mens der arbejdes på en løsning, orienteres brugerne om status på drifts nedbruddet via serviceportalen.
Opgave	○ Vis og forklar, hvordan Support Level 1 via ITSM kan informere brugere om driftsstatus. ○ Vis hvordan, brugere gøres opmærksom på, at der er driftsudfordringer. ○ Vis hvordan brugeren, kan se når der er ny status på en udmelding.

Service Level Agreement

Use Case	
Navn	Service Level Agreement
Formål	At demonstrere opsætning af Service Level Agreements.
Begyndelsesbetingelse	Systemejer henvender sig til Service Level Manager, fordi der er oprettet en ny IT-service.
Slutbetingelse	Nye SLA'er klar ved oprettelse af sag på IT-service
Forventet aktører	Service Level Manager, Systemejer, Configuration Manager
Forretningsregler	
Scenarie	101. Service Level Manager skal oprette 4 nye SLA'er til en ny IT-service. Systemejer har informeret Service Level Manager om Urgency på de enkelte SLA'er. - Der skal oprettes en SLA til Kritiske Fejl. - Der skal oprettes en SLA til Mindre Fejl. - Der skal oprettes en SLA til Ændringsønsker. - Der skal oprettes en SLA til Rådgivning og Customisering. 102. Service Level Manager logger på Systemet, og påbegynder processen. 103. Service Level Manager tager fat i de ansvarlige for hvert CI i IT-servicen, og aftaler en fornuftig OLA på de relevante CI's. 104. OLA skal altid indeholde "Tid Til Påbegyndt", og "Tid til Løst" for den enkelte type OLA. 105. Når der er indgået aftale om alle OLA'erne, opretter Service Level Manageren de 4 nye SLA'er med urgencies (Tid til Påbegyndt og Tid til Løst) på baggrund af OLA'erne. 106. Der signeres af på SLA'erne med systemejer. 107. Service Level Manager kontakter Configuration Manager og får vedkommende til at knytte de nye SLA'er til den nye IT-service 108. Service Level Manager validerer, at de nye SLA'er er tilgængelig, når der oprettes en sag på den nye IT-service. 109. Service Level Manager validerer at en sag eskaleres af Systemet, hvis en SLA brydes.
Opgave	19. Vis og forklar hvordan Systemet kan understøtte denne Use Case, med særligt fokus på ○ hvordan man angiver urgencies på OLA'er og SLA'er, ○ hvordan man tilføjer yderligere urgencies, ○ hvordan man tilknytter en SLA på en sag, ○ hvad der sker når SLA ikke overholdes.

Service Request

Use Case	
Navn	Service Request
Formål	At følge en sag fra start til slut, med alle handlinger.
Begyndelsesbetingelse	Bruger opretter sag via serviceportalen
Slutbetingelse	Support Level 1 lukker sagen
Forventet aktører	Bruger, Support Level 1
Forretningsregler	Support Level 1 er Single Point Of Contact (SPOC) Sagen skal altid lukkes af Support Level 1. Sager oprettes primært igennem Service Portal. Brugere må godt henvende sig til Support Level 1 support igennem telefon eller chat.
Scenarie	En bruger ringer til Servicedesk (Support Level 1). Support Level 1 er tilkoblet telefonsystemet, så Systemet åbner et sagsbillede med oplysninger om hvem der har ringet p.b.a. telefonnr. Brugeren forklarer at vedkommende ikke kan få Multifaktor Verificering til at virke. Support Level 1 benytter Service Request skabelonen til at oprette en Service Request, kategoriseret som Rådgivning ved MFA. Skabelonen indeholder en spørgeguide, som hjælper Support Level 1 med at få de rigtige oplysninger. Support Level 1 guider bruger igennem opsætning af MFA. Mens sagsbehandling foregår, er sagen låst for at andre kan redigere i sagen. Brugeren får aktiveret MFA, og Support Level 1 skriver i sagens løsningsfelt, hvad der er gjort, og afslutter sagen med korrekte løsningskode. Brugeren modtager en mail, med løsningsbeskrivelse og skal bekræfte, at hun er enig i, at sagen er løst. Support Level 1 modtager ikke nogen respons fra brugeren, så efter 7 dage lukkes sagen automatisk. Det er herefter ikke længere muligt at genåbne sagen.
Opgave	Vis og forklar, hvordan usecasen kan håndteres i ITSM. Herunder: ○ Oprettelse af sag ved telefon henvendelse. Søg bruger frem via AD. ○ Benyt en sagsskabelon. ○ Sæt korrekt kategori fra integreret liste. ○ Ved løsning af sag, skal der sættes en løsningskategori. Løsningen sendes til bruger. ○ Det skal fremgå af sagen, at den afventer godkendelse fra bruger. ○ Ved godkendelse skal Support Level 1, modtage en form for notifikation på, at bruger har godkendt løsningen. ○ Sagen lukkes med korrekt lukkekode.

	Vis og forklar, hvordan man nemt kan danne sig et overblik over sagen. ○ Sagsforløb, årsagsbeskrivelse og løsningsbeskrivelse skal stå separat og skal nemt kunne findes frem på sagen. Vis og forklar, hvordan man benytter en sagsskabelon. Vis, hvordan det kan ses, at sagen er låst for redigering og hvordan man kan se hvem der har låst sagen mod redigering og hvornår sagen blev låst.

Sikkerhedshændelse – bortkommen enhed

Use Case	
Navn	Sikkerhedshændelse – bortkommen enhed
Formål	At sagsbehandle en Sikkerhedshændelse i ITSM
Begyndelsesbetingelse	Bruger har fået stjålet sin PC
Slutbetingelse	Sag indberettet til datatilsynet indenfor pålagt tid.
Forventet aktører	Bruger, Support Level 1, Support Level 2
Forretningsregler	Der er 72 timer fra der opstår en Sikkerhedshændelse til at sagen skal være indberettet til datatilsynet.
Scenarie	Preben har i forbindelse med indbrud i hans hjem, fået stjålet sin arbejds computer. På computeren ligger der dokumenter med personfølsomme oplysninger.
Opgave	Vis, hvordan usecasen understøttes af ITSM. ○ Support Level 1 registrerer hændelsen via en blanket, hvor der er obligatoriske felter, der skal udfyldes. ○ Sagen får automatisk en høj prioritet via blanketten. ○ Efter Support Level 1 har behandlet punkter i blanketten, som hører til ved Support Level 1, sender Support Level 1 sagen videre til Support Level 2. ○ Support Level 2, får en notifikation om, at der er kommet en højprioritet sag til dem. ○ Support Level 2 kan ud fra informationer i blanketten oprette sag ved datatilsynet.

Styring af udlån

Use Case	
Navn	Styring af udlån
Formål	Styring af CI udlån, med integreret påmindelse om aflevering
Begyndelsesbetingelse	Udlån af CI, f.eks. pc. Udlånes af Support Level 1 og afleveres til Support Level 1
Slutbetingelse	Bruger har lånt pc og dette er registreret på brugerens profil
Forventet aktører	Bruger, Support Level 1
Forretningsregler	Der er mulighed for at låne diverse udstyr gennem Support Level 1
Scenarie	Søren har brug for at låne en LAB PC og sender derfor en anmodning via blanket på serviceportal. Support Level 1, modtager henvendelsen med alle nødvendige informationer, som er angivet i bestillingsformular. Support Level 1 gør udstyr klar og skriver til Søren, når udstyr er klar til afhentning. Søren "underskriver" for udlevering via serviceportalen Ved udlåns ophør, modtager Søren en påmindelse fra ITSM om at udstyr skal afleveres. Søren glemmer at aflevere udstyr til tiden, så ITSM sender automatisk en påmindelse om at udlånstiden er overskredet. Søren afleverer udstyr og "underskriver" for aflevering.
Opgave	Vi og forklar hvordan ITSM understøtter Use Casen med særlig fokus på: ○ Registrering af anmodning om udlån ○ Udlevering af udlån ○ Påmindelse om snarlig aflevering ○ Påmindelse ved for sen aflevering ○ Mulighed for underskrivelse ved modtagelse og aflevering