



PRELIMINÄR RISKANALYS ENLIGT NIS2, HAZID & HAZOP

Riskanalys gör du varje dag: Klar med frukost dags för jobbet. Du tittar ut, snöoväder: halka, frysa, krocka, försening. Det blir dunjacka och vinterkängor. Du har gjort en första riskanalys i projektet ta sig til jobbet.



ULF DELLBORG



PODD



PRELIMINÄR RISKANALYS PÅ 2 MIN

En riskanalys är meningslös om den inte säkrar den samhällsviktiga funktionen. Ension allriskansats (Människa, Process, Teknik, Miljö) i en preliminär riskanalys är första steget mot cybervärdighet och skydd av de samhällsviktiga system.

Genom en initial screening hittar vi verksamhetens högriskområden. Resultatet ger er kontroll: ni ser om ni omfattas av cybersäkerhetslagen och vet exakt vilka delar som kräver djupare analys för att skydda både samhället och era intäkter. Den preliminära riskanalysen utgör steg 1 i en komplett [riskanalys för cybersäkerhet enligt NIS2](#).

INNEHÅLL

VAD ÄR RISKANALYS CYBERSÄKERHET

METOD PRELIMINÄR FARO OCH RISKANALYS

1. IDENTIFIERA TJÄNSTERNAS FAROR, HAZID

2. DEFINIERA SAMHÄLLSVIKTIGA TJÄNSTER

3. KRITISKA PROCESSER & VIKTALLOKERING

4. RISKANALYS AV FAROR INIFRÅN (HAZOP)

5. SYNTES AV HAZID & HAZOP

6. FASTSTÄLLA RISKNIVÅ OCH PRIORITERA

Säker arkitektur, lösningen på säkerhetskraven

Den här artikeln berättar hur du gör en preliminär faro och riskanalys. Syftet är att i en förstudie, kontextanalysen, identifiera riker med det du tänker införa.

Jag vänder mig till dig som leder eller ska genomföra arbetet. Du ska förstå vad standardiserade metoder kan hjälpa dig med efterlevnad av cybersäkerhetslagen. När du gjort detta kan du fokusera på rätt system och rätt policys. Detta är grunden för cybersäkerhet genom desired paths. Processen kan anpassas efter era behov

VAD ÄR RISKANALYS CYBERSÄKERHET

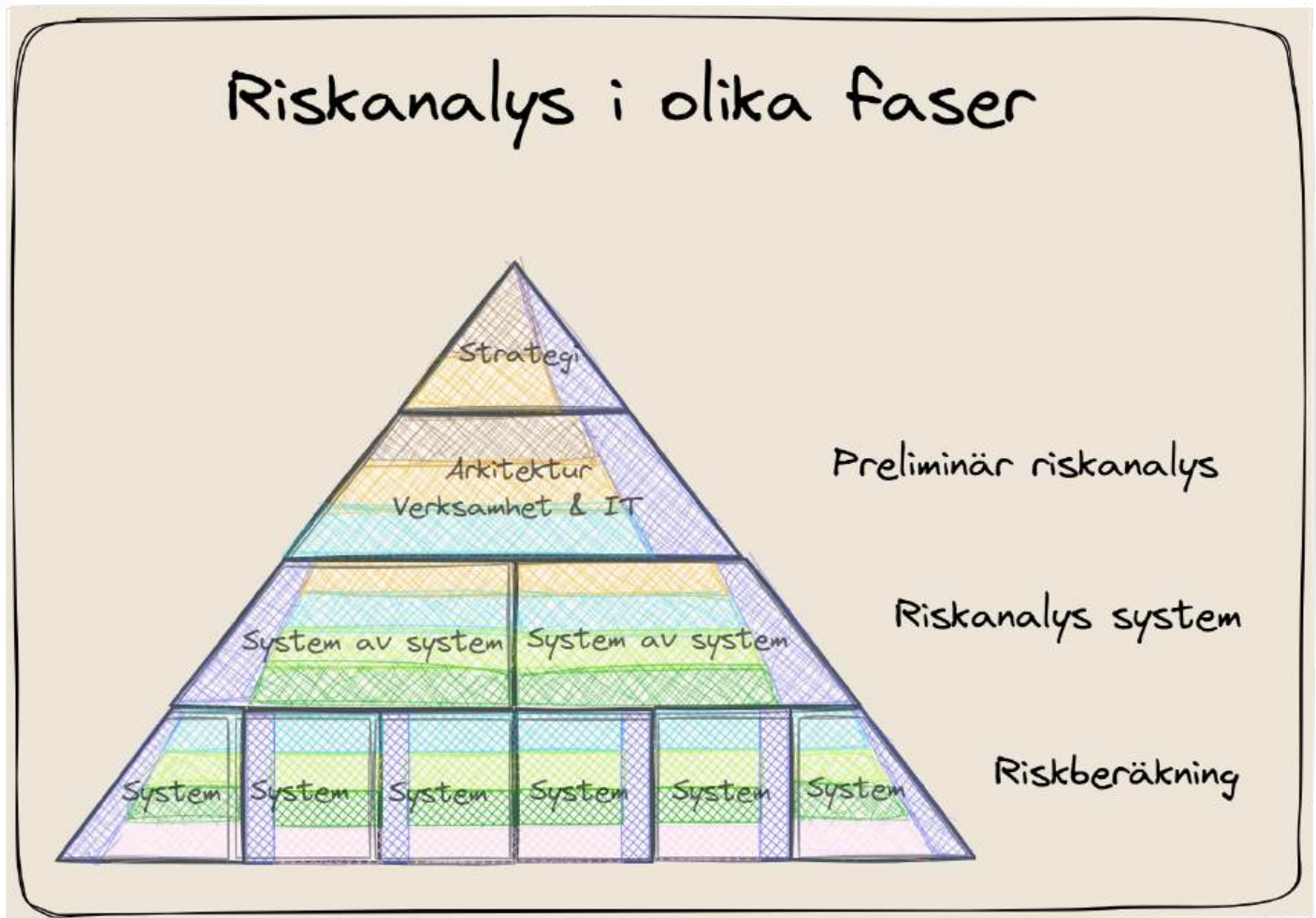
Cybersäkerhetslagens / NIS2 krav på riskanalysen är ett allriskperspektiv (All-hazards approach)



Cybersäkerhetslagen kräver att samhällsviktiga tjänster fungerar. Riskanalysen ska göras med en allriskansats, Din affärsmodells tjänster är ditt fokus.

NIS2 krav på riskanalys framgår av EU-kommissionens genomförandeförordning. Det innebär att detta även blir cybersäkerhetslagens krav. Den är lik den riskanalys för informationssäkerhet som finns beskriven i ISO 27001 och ISO 27005.

LÄS MER OM CYBERSÄKERHETSLAGENS KRAV



Genom de detaljerade reglerna för riskhantering krävs rent praktiskt att tre olika metoder följs, i grunden sätter genomförandeförordningen kraven, kraven där är strukturellt lika ISO 27001, men krav sätts även på en säker systemutvecklingscykel (SDLC), här safety & security by design. Det leder till att nyttja IEC 61508.

De sammanlagda kraven innebär praktiskt att du först måste göra en preliminär riskanalys, detta innan du teknisk designar ditt system. Sedan måste du göra en riskanalys för att uppnå rätt systemdesign.

ANSSI:s metod EBIOS Risk Manager

Franska ANSSI gör samma uppdelning. Deras metod EBIOS Risk Manager börjar i verksamhetens värden. Farliga händelser identifieras, var och en med bedömd allvarlighetsgrad, och sedan byggs händelsekedjorna fram till dem – först på verksamhetsnivå, därefter genom tekniken. Skillnaden är att EBIOS är inriktad på avsiktliga angrepp. Cybersäkerhetslagen kräver att funktionen upprätthålls oavsett orsak.

Enson gör därför en enda process av två som annars går parallellt: systemdesign enligt ISO 15288 och ISO 9001, och safety och security by design enligt genomförandeförordningen, IEC 61508 och ISO 27000-familjen. Utgångspunkten är affärsmodellen, och slutpunkten är ett

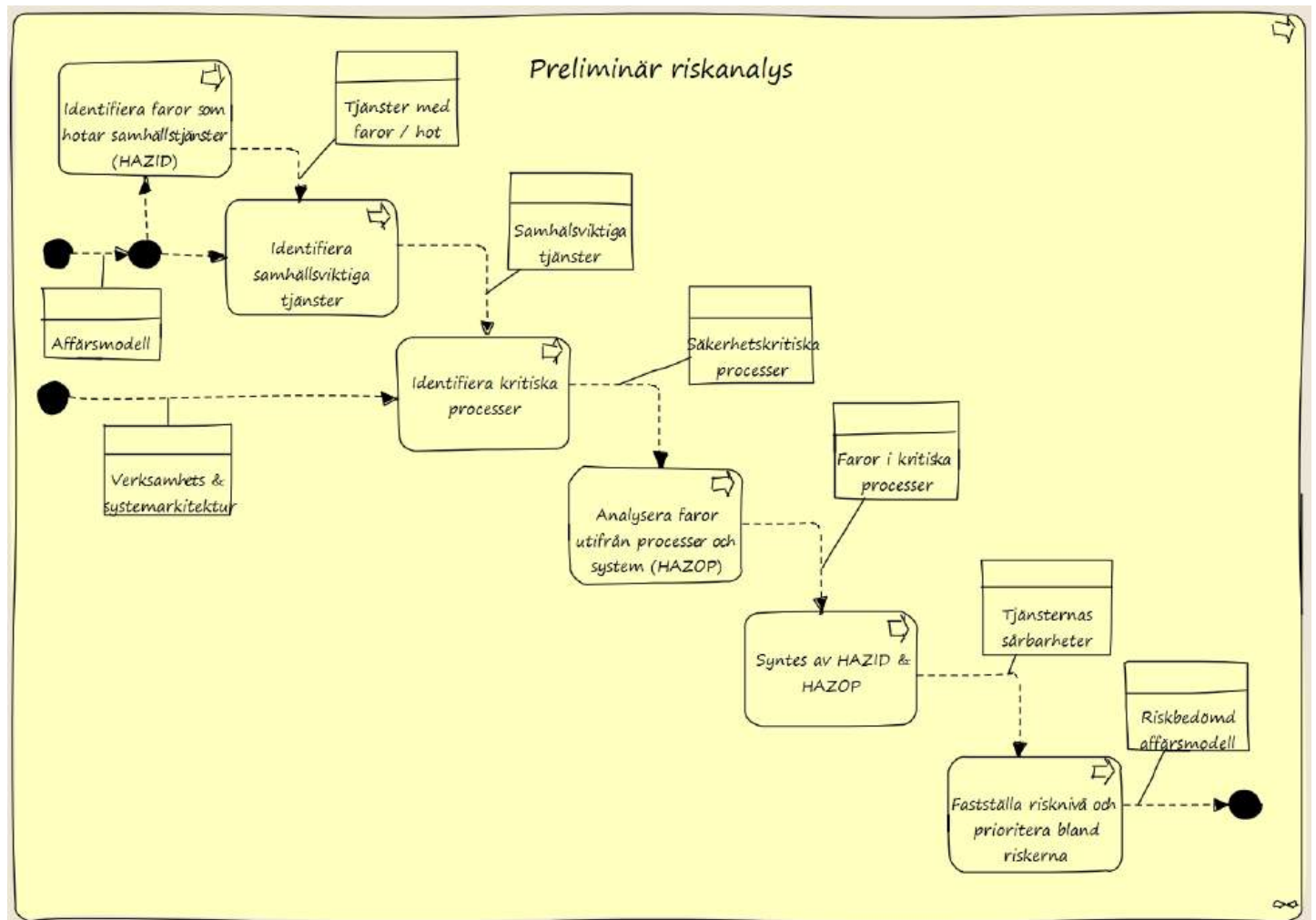
system som går att bevisa säkert.

- Jämförelse: Riskanalys enligt Cybersäkerhetslagen – Ension vs. Traditionella metoder

+

HAZID OCH HAZOP: METODER FÖR SYSTEMATISK RISKIDENTIFIERING

Process för preliminär riskanalys ur ett allriskperspektiv



Preliminär faro och riskanalys görs i tidigt. Du identifierar övergripande risker och utgår från affärsmodellen:

1. HAZID-analys. Identifiera de faror som kan uppstå.
2. Bestäm vad som är samhällsviktigt i affärsmodellen.
3. Identifiera säkerhetskritiska processer
4. HAZOP-analys av processer och systemarkitektur för att hitta orsaker till farliga händelser.
5. Syntes av HAZID & HAZOP, en sammanvägning.
6. Fastställs risknivå och prioritera riskerna. Detta skapar en riskmatris med prioriteringen av riskerna.

HAZID och HAZOP är metoder för riskanalys:

HAZID (Hazard Identification) och HAZOP (Hazard and Operability Study) är två fundamentala metoder för att säkra komplexa system. Ension använder dessa i den preliminära riskanalysen för att fånga risker ur ett allriskperspektiv:

- HAZID är en bred screening. Syftet är att göra en övergripande riskidentifiering för att sätta ramen för säkerhetsåtgärder och policy. Vi identifierar de yttre hoten (brand, strömavbrott, hackers) för att veta vad vi ska skydda. Fokus är risker ur ett allriskperspektiv. Du tittar på systemet utifrån som en black box.
- HAZOP är en detaljerad analys av processerna. Vi identifierar systematiska fel i processen (vad händer om data uteblir eller är felaktig?) för att veta hur vi ska skydda det. Fokus är att bedöma driftsproblem. Analysen kräver specifikation av verksamhets och systemprocesser.

Båda bygger på tvärfunktionellt teamarbete och systematiska guideord för att identifiera faror. allriskperspektivet står i centrum och guideord hjälper dig i en allriskansats. Nu har AI klivit in i teamet och kan hjälpa dig.

1. IDENTIFIERA FAROR OCH RISKER FÖR AFFÄRSMODELL OCH SAMHÄLLE (HAZID)

1.1. HAZID, en riskanalys att Identifiera faror och risker



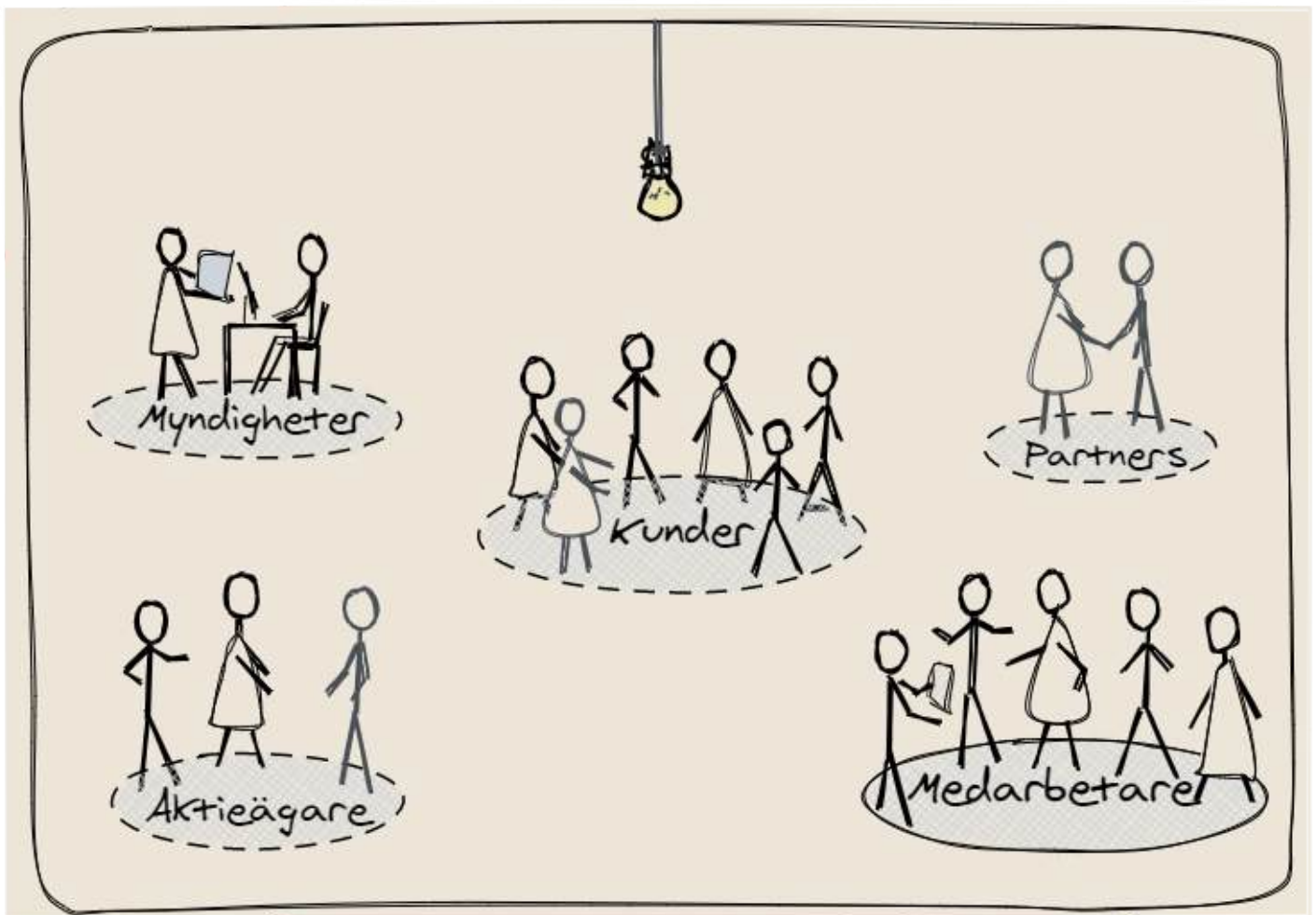
HAZID (Hazard Identification), identifiering av faror, är en riskanalys för att identifiera potentiella faror och hot. Syftet är att i ett tidigt skede för att säkerställa att säkerhetsarbetet beaktar trovärdiga farliga scenarier.

Att tänka på i arbetet innan du startar riskanalysen

- Tänk utanför boxen och betrakta din verksamhet ur olika perspektiv.
- Involvera olika avdelningar: IT, säkerhet, drift, etc.

- Följ med i de senaste trenderna inom hot.

1.2. Resurser för riskanalys med HAZID

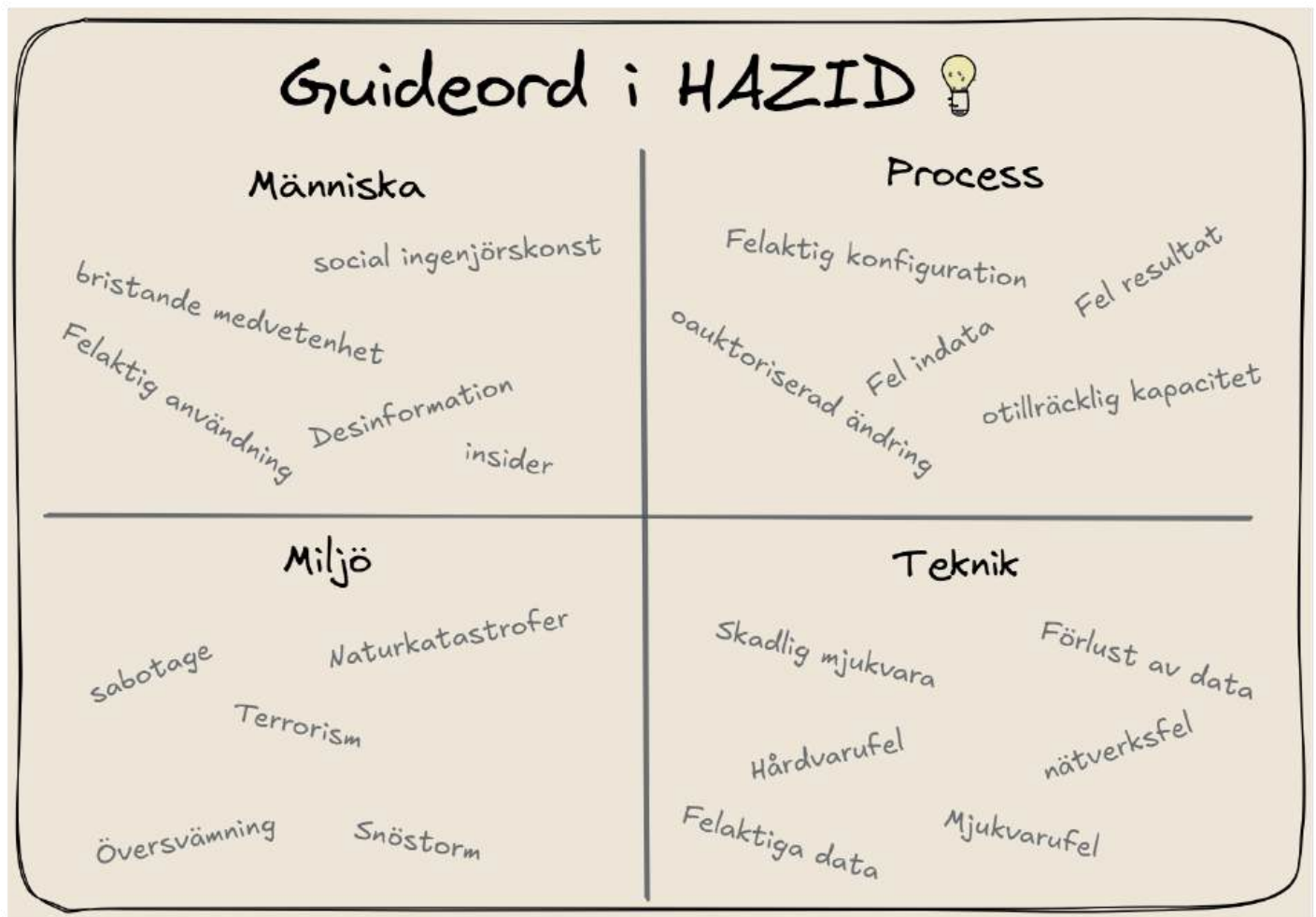


Ledaren bör ha god kunskap om cybersäkerhet samt förstå risker förknippade med samhällsviktiga tjänster.

Sekreteraren bör ha teknisk bakgrund inom IT-säkerhet.

Gruppen bör inkludera experter inom affärsmodell, IT, säkerhet, juridisk och kommunikation. Kunskap om attacker riktade mot samhällsviktiga tjänster är mycket bra. Involvera andra organisationer som t.ex. kunder, partners och myndigheter.

1.3. Stödord för riskanalys enligt HAZID för cybersäkerhet

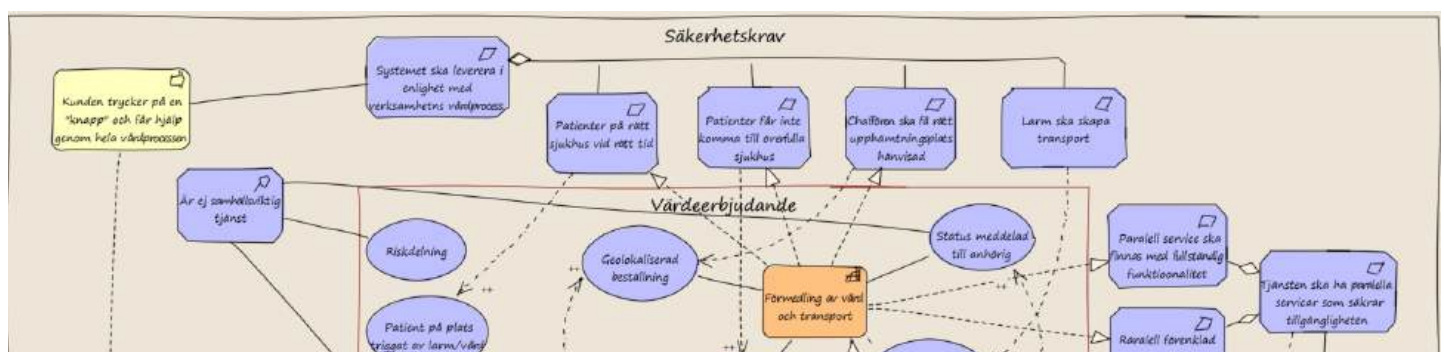


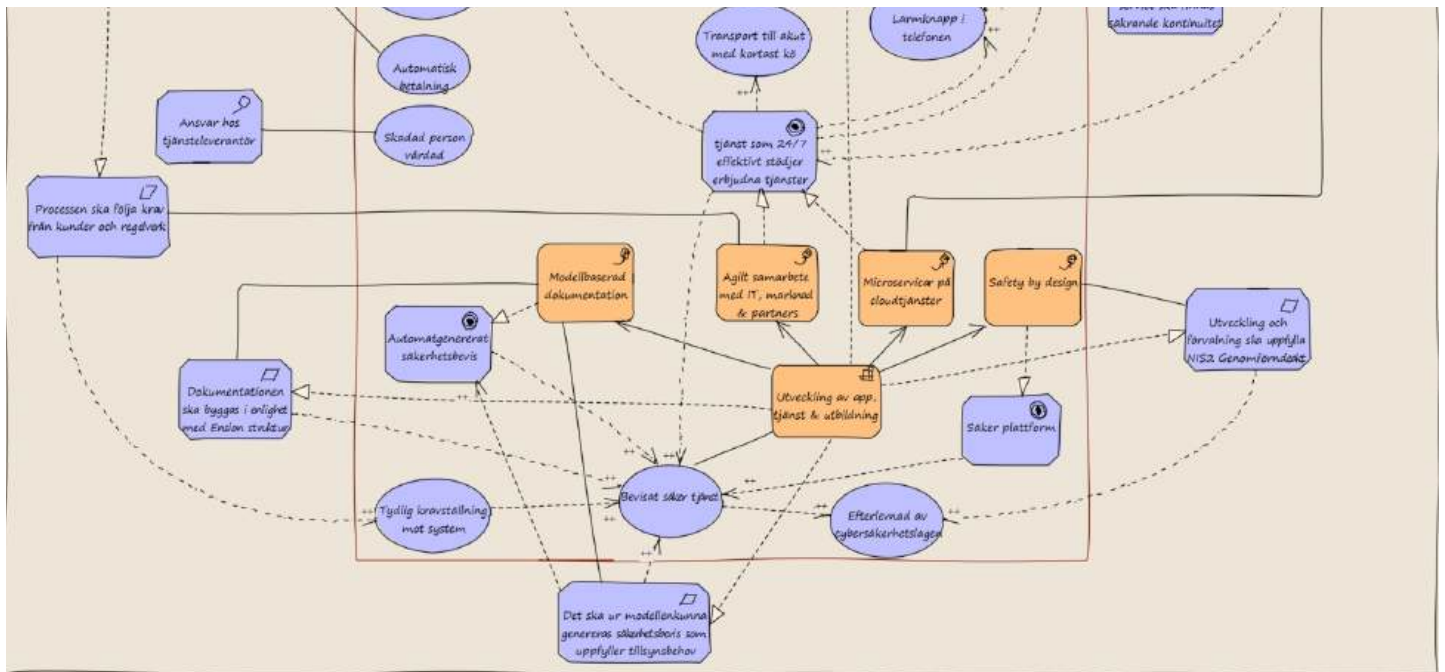
När en HAZID för cybersäkerhet ska genomföras och guideorden anpassas. Grundläggande guideord:

- Människan: Felaktig användning, bristande medvetenhet, social ingenjörskonst, insiderhot.
- Process: Felaktig konfiguration, bristande uppdateringar, obehörig åtkomst, dataförlust.
- Teknik: Hårdvarufel, mjukvarufel, nätverksfel.
- Miljö: Naturkatastrofer, sabotage, terrorism.

Använd guideorden i AI-arbetet samt innan och i workshopen för att skapa scenarier och kreativitet.

1.4 Underlag för HAZID-analysen





Underlaget som ska tas fram innan AI gör sin analys och som sedan skickas till intressenterna tillsammans med HAZID med hjälp av AI är följande.

- Affärsmodell med SWOT-analys,
- Intressentanalys med säkerhetskrav
- Anpassade guideord som passar er analys
- Rapporter från tidigare cyberattacker & incidenter
- Scenarier baserat på t ex punkterna ovan. Använd AI för att skapa både scenarier och skapa poddar med NotebookLM om varje sceario.

► P O D D F Ö R S C E N A R I O T

1.5 AI i tre steg tar fram kandidatfaror

AI spelar roller tre steg:

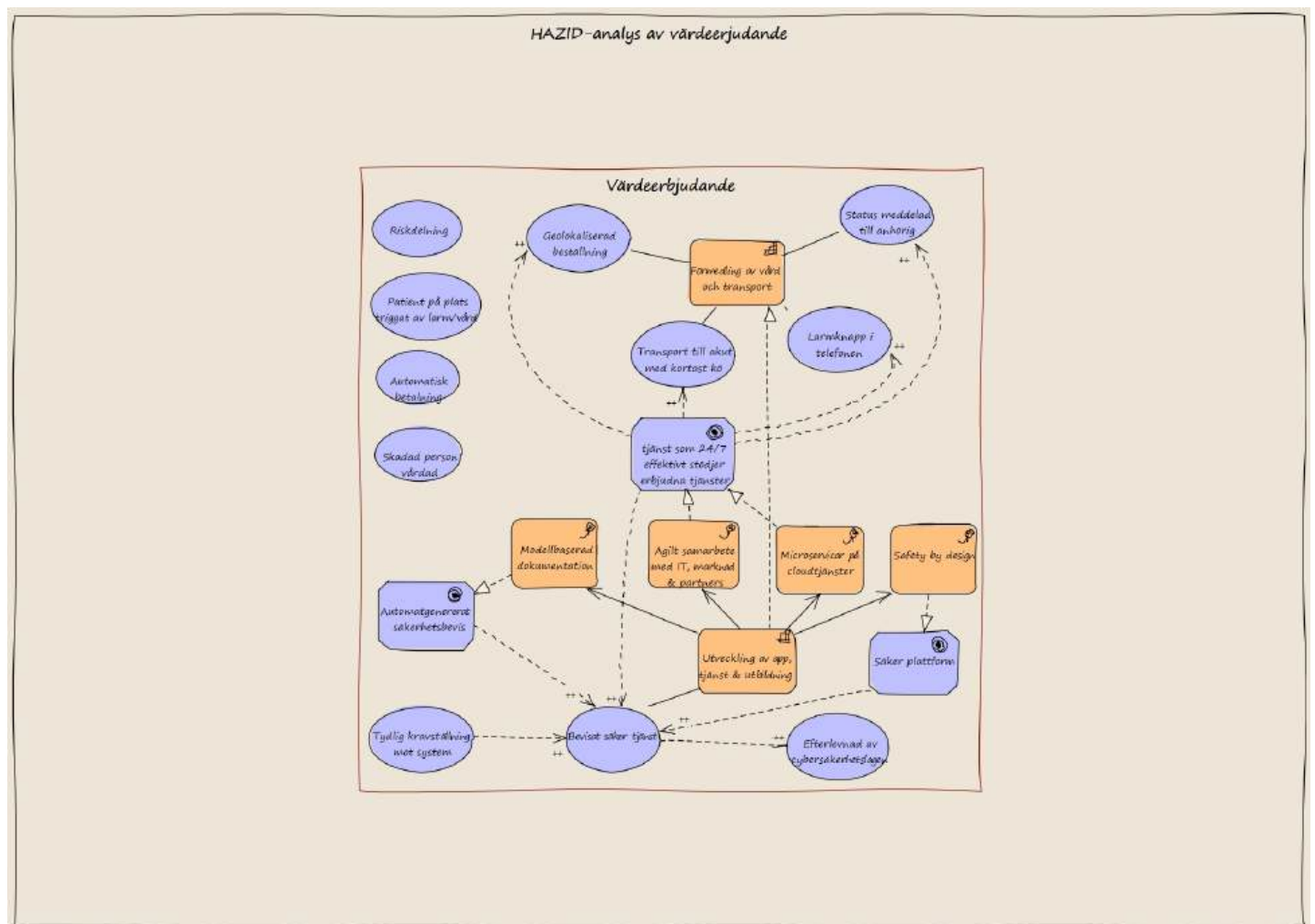
1. **AI-intressenternas säkerhetsanalytiker** gör varsin HAZID med stödord och annat underlag som grund.
2. **AI-säkerhetsanalytikern** sammanställer ai-intressenternas resultat till ett diagram.
3. **AI-angriparen** försöker hitta på djävulskap, varför inte ett hybridhot eller två.

Idén med HAZID är att med guideord ge idéer om hur faror kan uppstå i verksamheten. Men hundra kombinationer av guideord orkar ingen gå igenom. Det orkar däremot AI. Och AI är dessutom bra på rollspel.

Som arkitekt får du hjälpa AI med att bygga modell: avvikelser och förlopp som Business Events, kopplade till informationsobjekten och processteg. Resultatet avvikelseerna leder till dokumenteras som Outcomes, de kända från HAZID återanvänds, nya läggs till. Och tänk på, modellen är hela tiden facit

- **Prompt 1: AI-intressenternas säkerhetsanalytiker gör HAZID** +
- **Prompt 2: AI-säkerhetsanalytikern sammanställer intressenternas resultat** +
- **Prompt 3: AI-angriparen angriper diagrammet** +

1.6 Inför Workshop HAZID



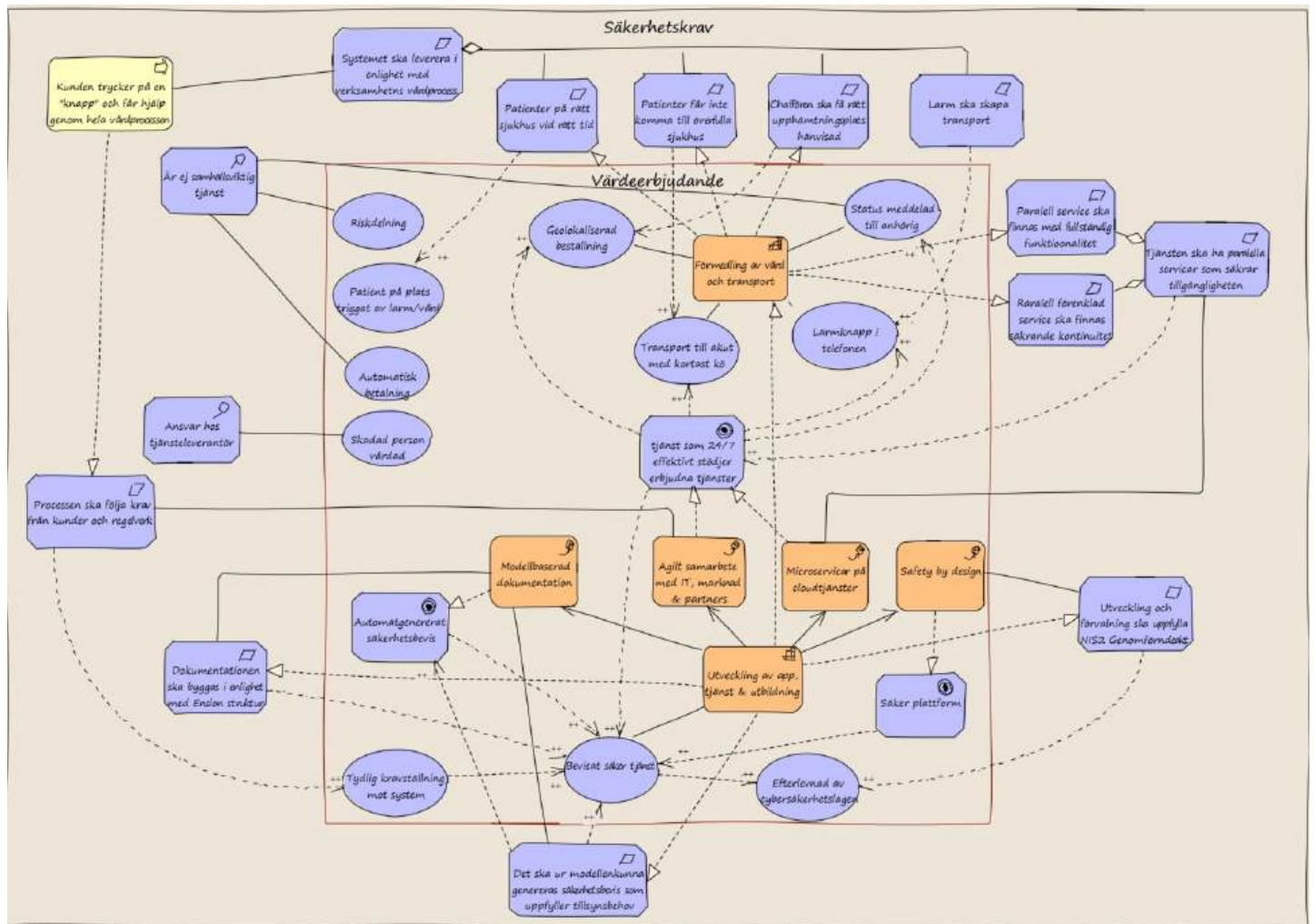
Material på gemensam whiteboard

- Diagrammet,
- Lista med öppna frågor
- Scenariopoddar, berättelser om organisationens verksamhet
- Riskanalysen en överblickspodd

Poddarna finns för att tvinga fram långsamt tänkande innan workshopen. En lista på en skärm skummas av System 1. En berättelse i öronen kan inte skummas, den tar sin tid, och under tiden börjar deltagaren invända.

Innan diagrammet öppnas skriver varje deltagare ner tre farliga händelser utifrån sin egen erfarenhet. Ofta kommer de tre farorna direkt ur det som gnagde under poddlyssningen. Därefter granskas diagrammet utifrån vad som inte finns med.

1.7. Workshop HAZID: gallra, komplettera, kedja



Börja med att presentera av övergripande så alla förstår föremålet för analys. Håll mötet ganska kort.

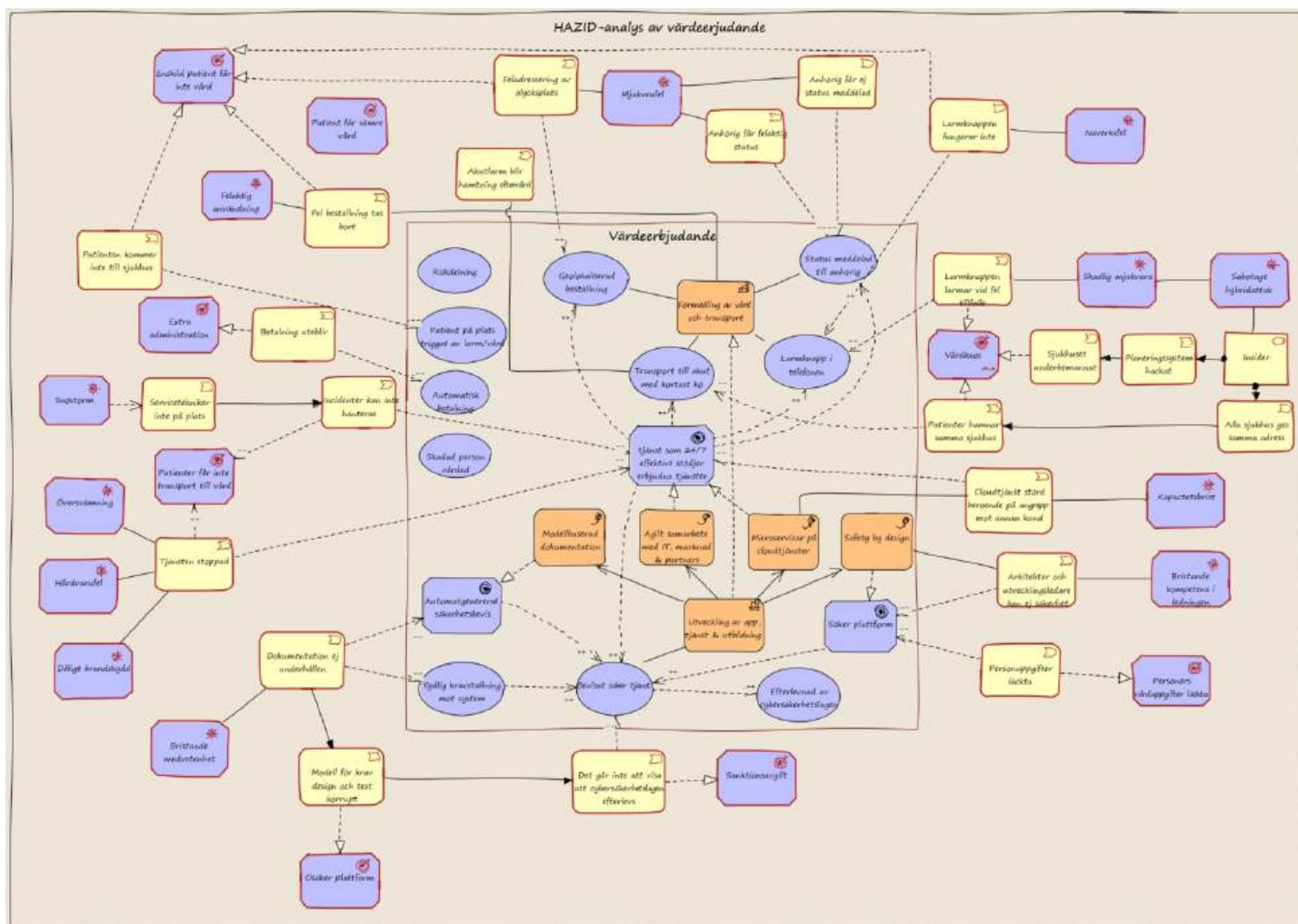
- 10 min, presentation av syfte, avgränsning och metod
- 15 min De egna farorna. Varje deltagare presenterar sina tre, medan uppmärksamheten är som störst.
- 20 min Där rollerna är oense. Avsnitt C ur sammanställningen. Här ligger de verkliga luckorna.
- 15 min Gallring. Vilka kandidater är inte trovärdiga
- 20 min Kedjor. Håller de kedjor AI byggt?
- 15 min Hybrider. Avsnitt D, plus det teamets egna.
- 5 min sammanfattning

Facilitatorns tre uppgifter.

1. Se till att gallringen faktiskt sker; grupper är obekväma med att stryka, och en lista ingen tror på slutar användas.
2. Se till att drift- och supportfolk hörs, de vet hur systemen beter sig i verkligheten.
3. Låt inte diskussionen glida in i tekniska lösningar; det är inte det här steget.

Vid stort scope delas workshopen i två: en för oenighet och gallring, en för kedjor och hybrider.

1.8. Formalisering i modellen



Efter workshopen uppdateras modellen baserat på resultatet på den digitala tavlan.

Relationer är det som avslöjar att två faror egentligen är samma, att en kedja saknar ett led, eller att ett resultat inte träffar något värde. En outcome utan koppling till ett värde betyder antingen att resultatet inte spelar någon roll, eller att kontextanalysen missat ett värde.

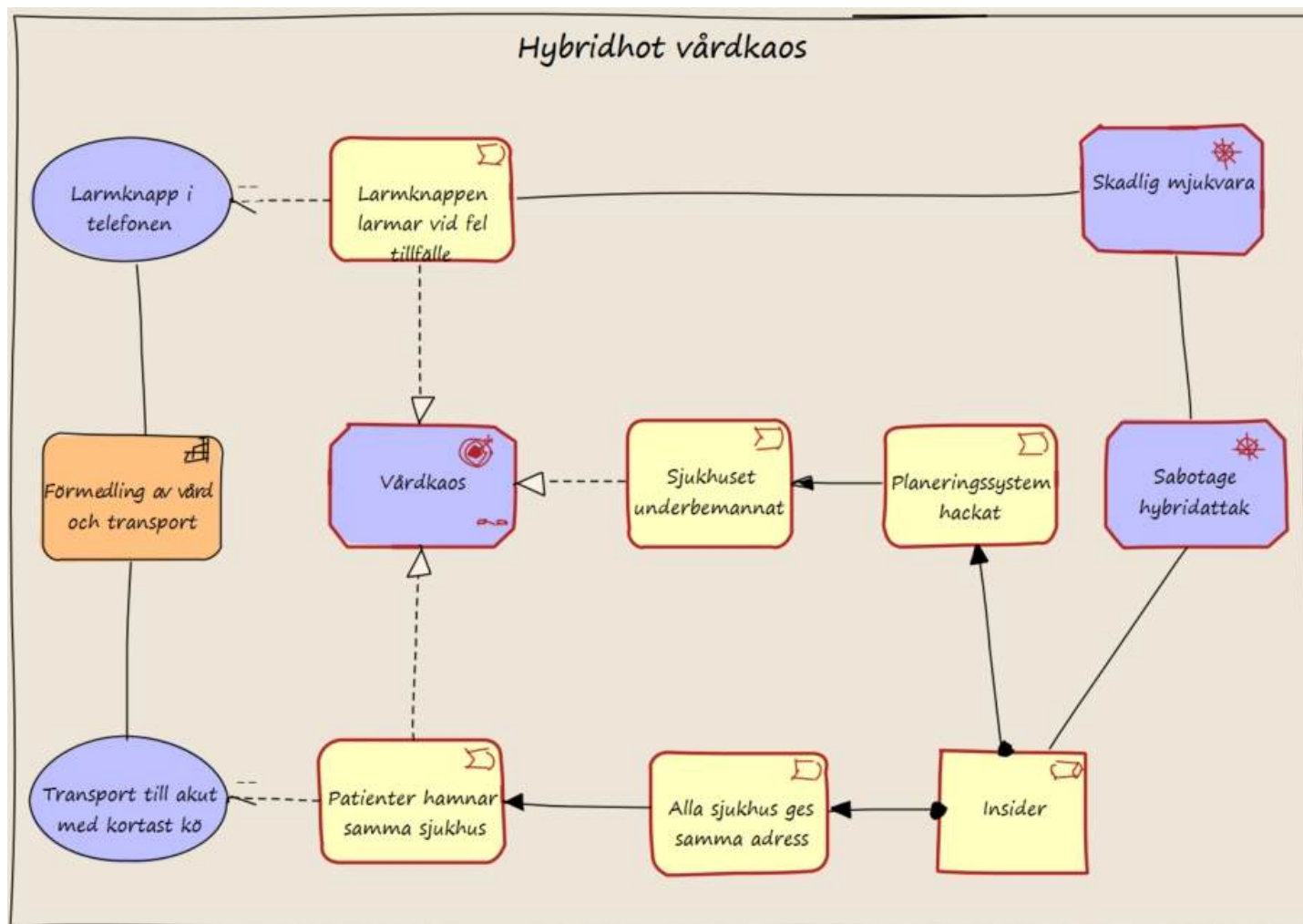
Öppna frågor markeras som öppna på whiteboarden med instruktioner till teamet och kallelse till en ny workshop..

Hazid-analys för Gipsat.nu

2. IDENTIFIERA SAMHÄLLSVIKTIGA TJÄNSTER

2.1. Skapa beslutsunderlag med riskscenarier

HAZID-arbetet i kapitel 1 gav en modellerad bild av vad som kan gå fel. Nu ska den användas för att besluta vilka tjänster som är samhällsviktiga. Scenarierna är bästa underlaget, de visar konsekvensen i stället för att beskriva den.

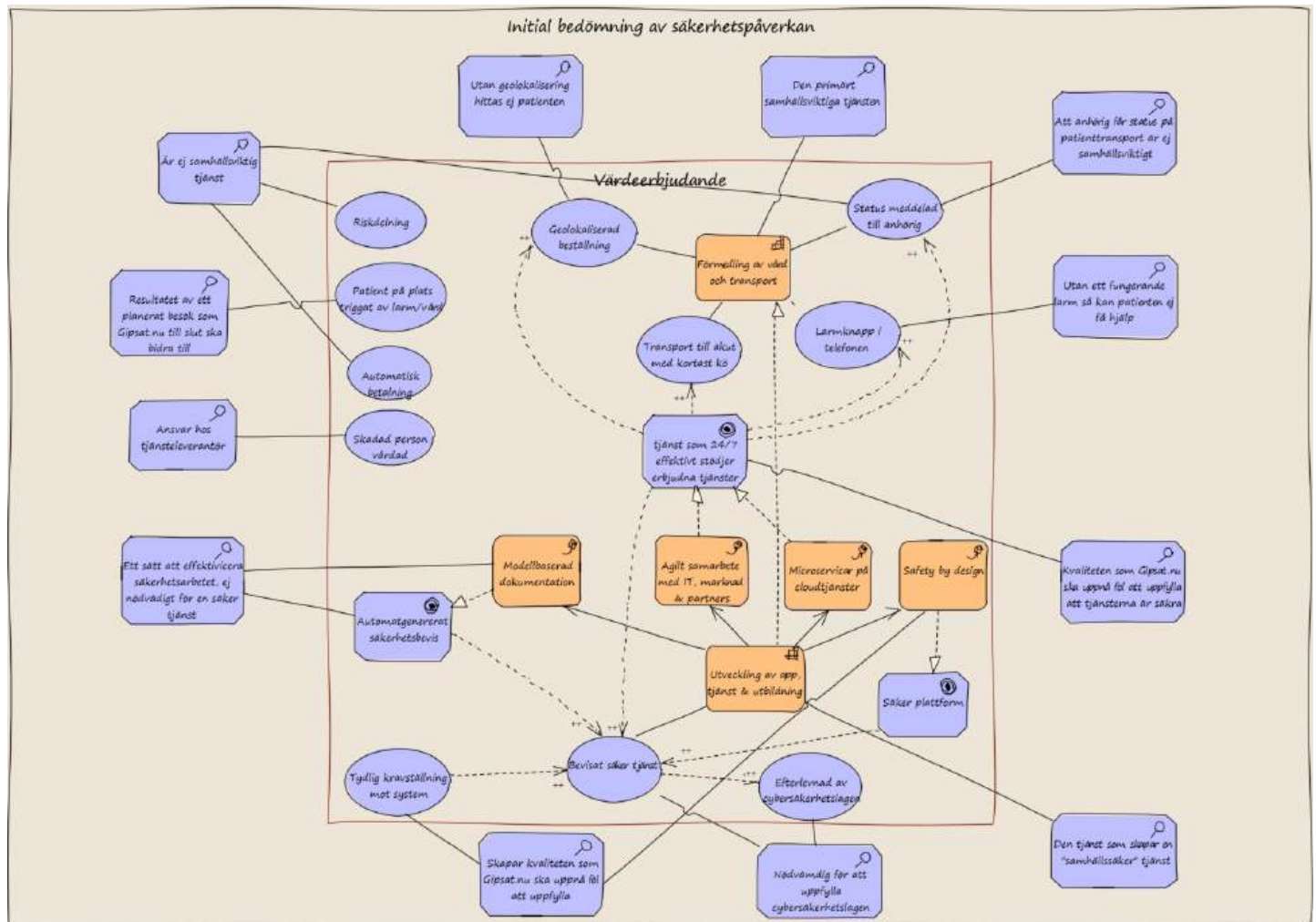


En hybridattack sker mot Gipsat.nu, vårdens uber:

- Alla sjukhus ges samma fysiska adress så alla körningar av skadade hamnar på samma sjukhus.
- Planeringssystemet hos sjukhuset som de skadade kommer till är hackat så det är underbemannat
- Kundernas telefoner har en malware så att telefonerna larmar utan att kunden tryckt på knappen.

Resultat: Överbelastat sjukhus och falska vårdkörningar.

2.2. Workshop för att bedöma vilka tjänster som är kritiska



Här görs en bedömning av vilka tjänster som är kritiska, beslutet är ledningens. Dagordning för workshopen.

- 15 min. Genomgång av HAZID och scenarierna.
- 20 min. Bedömning per tjänst enligt riskkriterierna.
- 15 min. Beslut om vilka tjänster som går till kapitel 3.
- 5 min. Riskbeslut. beslutade samhällsviktiga tjänster

Det är här ni bekräftar eller justerar viktningen av värden från kontextanalysen. Den var en hypotes byggd på affärsförståelse; nu har ni analysen. Resultatet städas och skickas ut efter workshop.

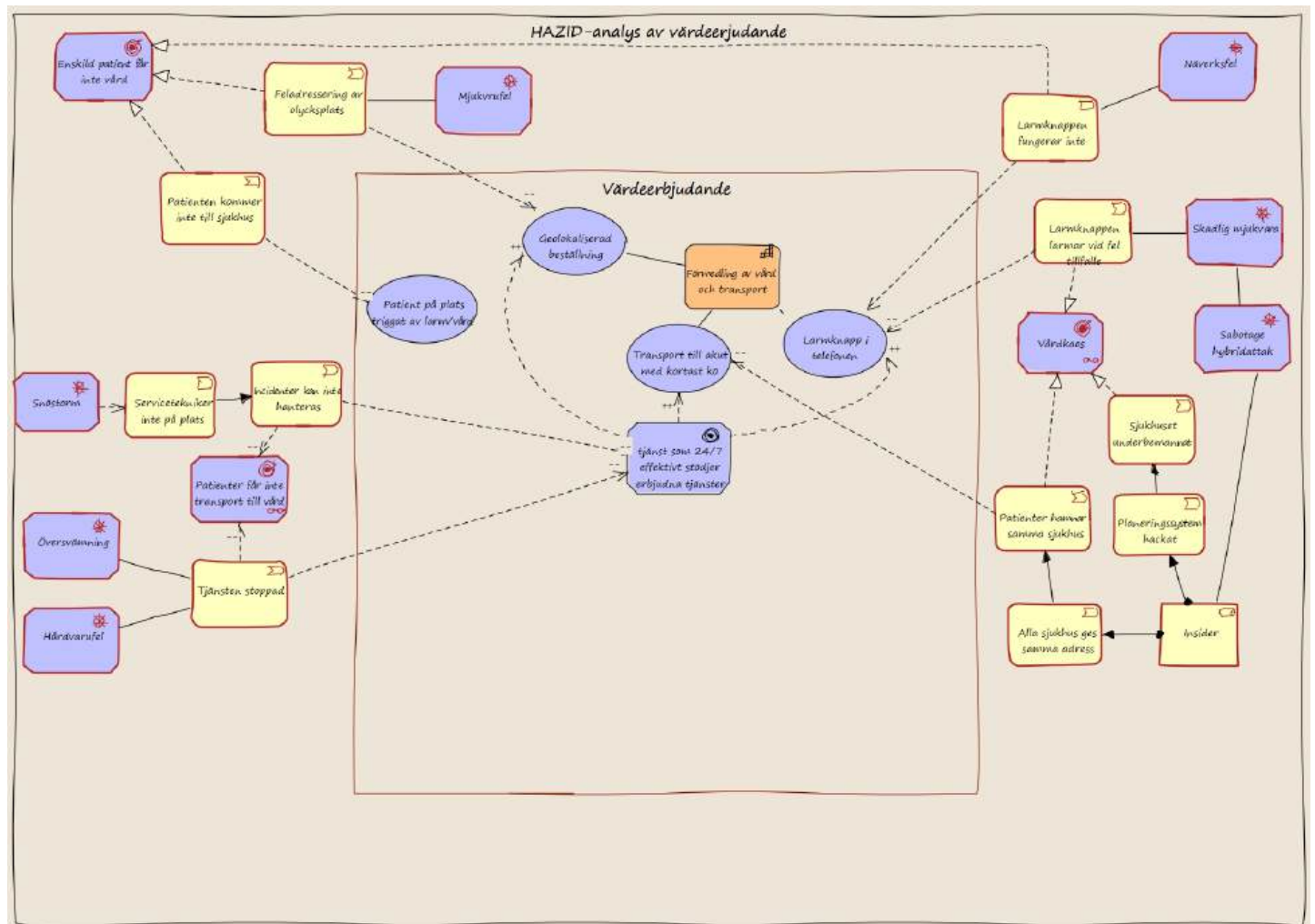
- Viktade värden för Gipsat.nu

+

2.3. Viktningen hos det totala värdeerbjudandets förmågor

Ledningen känner igen förmågor, det är dessa som finns i affärsmodellen och intressentanalysen. En förmåga implementerar en eller flera värden. Förmågan får vikten efter värdet med den högsta vikten. Redovisa sedan förmågorna som profiler, vilka vikter implementerade värden har och förmågans resulterande vikt.

2.4. De samhällsviktiga tjänsterna



Samtliga resultat pekar mot samma förmåga och samma values i värdeerbjudandet: förmedling av vård och transport med geolokaliserad beställning, transport till akut med kortast kö, larmknappen som utlöser flödet. Transport triggat av larm utförs av partnern taxi.

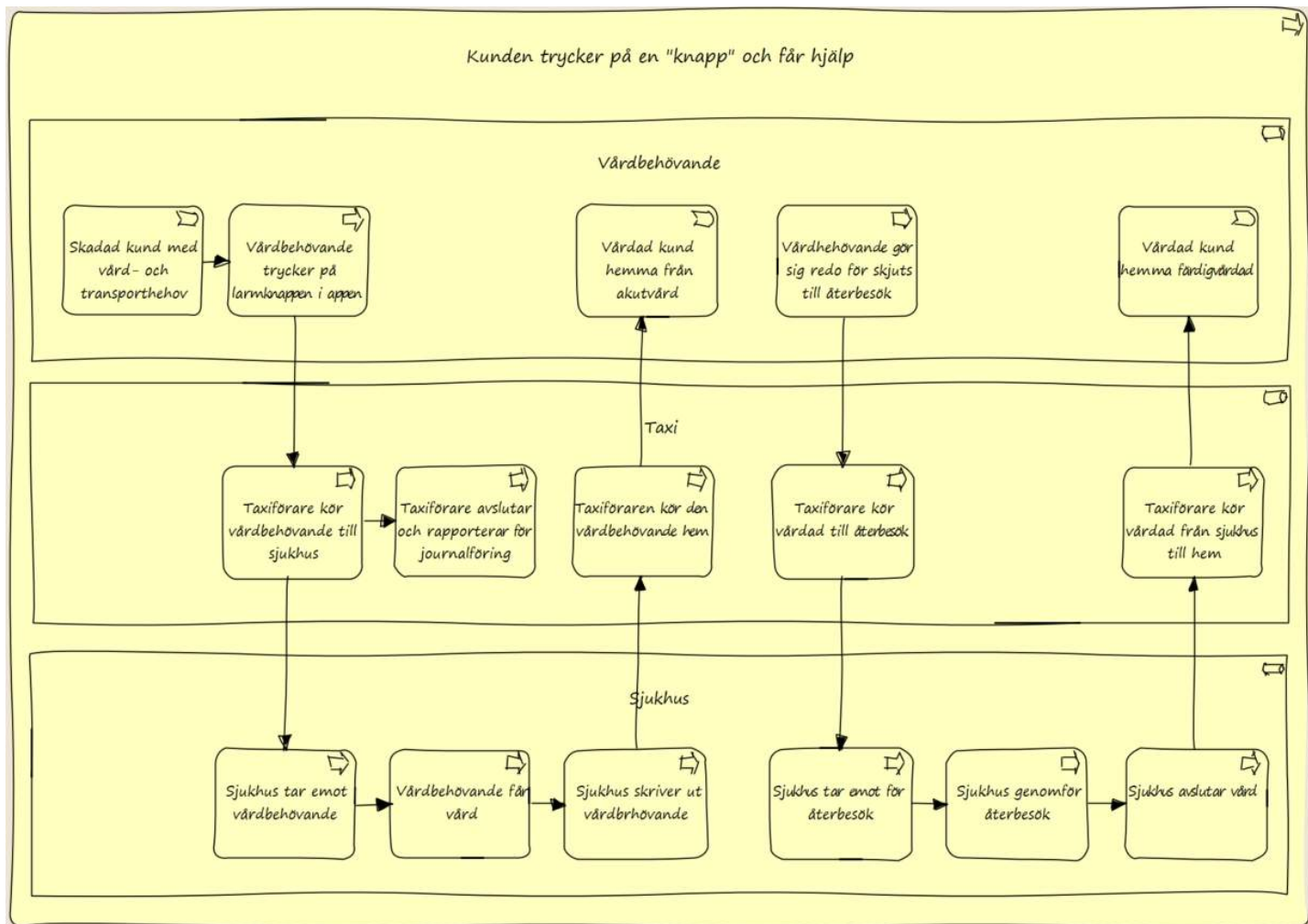
Övriga values i erbjudandet har inga resultat riktade mot sig. Slutsatsen är att förmedling av vård och transport är den samhällsviktiga tjänsten, en gallring som kommer ur analysen, inte ur en bedömning av vad som känns viktigt.

3. IDENTIFIERA SÄKERHETSKRITISKA PROCESSER OCH ALLOKERA VIKT

HAZID-analysen visar vilka outcomes som hotar vilka delar av erbjudandet. För Gipsat pekar "patienten kommer inte till sjukhus", "patienter får inte transport till vård" och "vårdkaos" alla mot samma värden: förmedling av vård och transport. Det är den samhällsviktiga tjänsten.

Inför detta steg vet du vilken tjänst som är kritisk, och processen som krävs för att leverera tjänsten. Men du vet inte vilken del av processen som är säkerhetskritisk, vet du det kan du navigera dig fram till säkerhetskritiska system.

3.1. Kartan över de viktiga tjänsterna ger de säkerhetskritiska processen.



Processbilden här visar hela vårdprocessen: akutflödet, hemtransporten, återbesöket och avslutningen. Alla fyra realiserar erbjudandet, Nu skall du ska du ta reda på vilka processteg som är säkerhetskritiska.

I kontextanalysen viktade ledningen vad som är kritiskt på en skala 1–5, där 5 betyder noll tolerans för att processen inte fungerar.

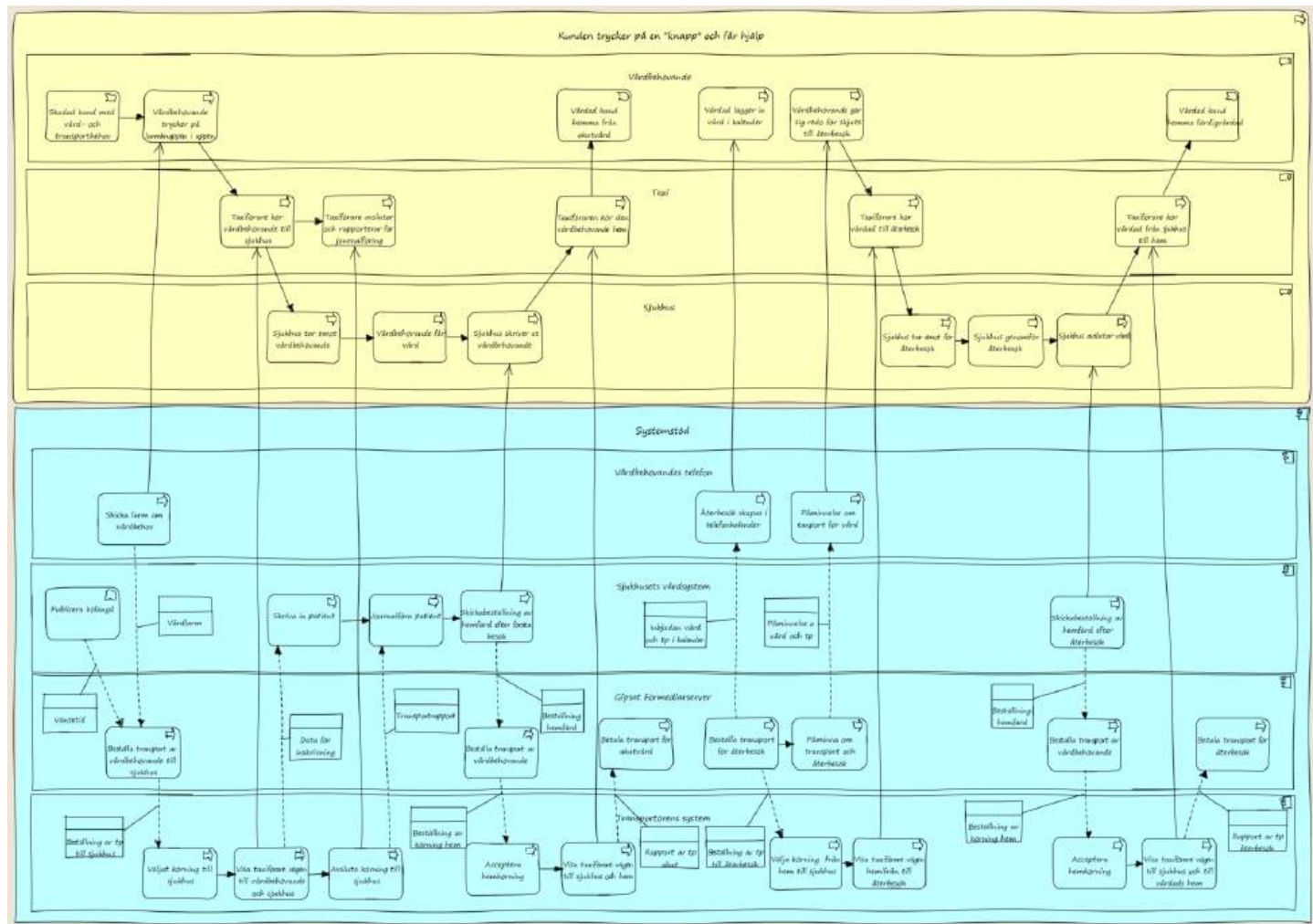
Första steget är att vikta stegen i verksamhetsprocessen. Det görs nedan, men för gipsat.nu inses det lätt att akutflödet är viktigast, de första fem processtegen.

3.2. Hitta kritiska huvudspår i affärsprocessen

Försök dela upp processen i större delar. Gipsat.nu kan dela vårdprocessen i fyra delar: akutflödet, hemtransporten, återbesöket och avslutningen. Alla fyra realiserar erbjudandet. men de har olika kritikallitet. Tre frågor skiljer dem åt.

1. Vilka outcomes från HAZID träffar delen? Det är den hårdaste frågan, eftersom svaret kommer ur analysen och inte ur en bedömning.
2. Hur snabbt måste den fungera? Det är tidskravet som gör en tjänst samhällsviktig, inte innehållet. Samma tjänst kan vara kritisk i ett flöde och trivial i ett annat.
3. Vad kostar en väntan? Om det finns en väg runt, hur mycket sämre blir utfallet med den?

3.3 Från verksamhetsprocess till säkerhetskritisk process



Processbilden har två halvor. Den gula visar vad människor gör, den vårdbehövande larmar, taxiföraren kör, sjukhuset tar emot. Den blå visar processen i systemstödet: användarappen, förmedlarservern, chaufförsappen och sjukhusintegrationen.

Det är den blå halvan som ska analyseras i HAZOP, eftersom det är där de systematiska felen uppstår. Men vikten kommer från den gula, för det är där värdet levereras. Det är dessa vikter ni använder när ni i 3.6 identifierar den säkerhetskritiska processen.

3.4 Förberedelser inför workshop och enskild bedömning

Första steget är att skapa ett underlag för workshopen så att deltagarna kan förbereda sig. Prompten kopplar ihop verksamhetslager och applikationslager och beskriver vad ett bortfall skulle innebära. Den föreslår ingen vikt. En siffra i underlaget gör att deltagarna bedömer om AI:s siffra i stället för att själva bedöma steget.

- Prompt: AI skriver bedömningsunderlaget

- Tabell för utskick

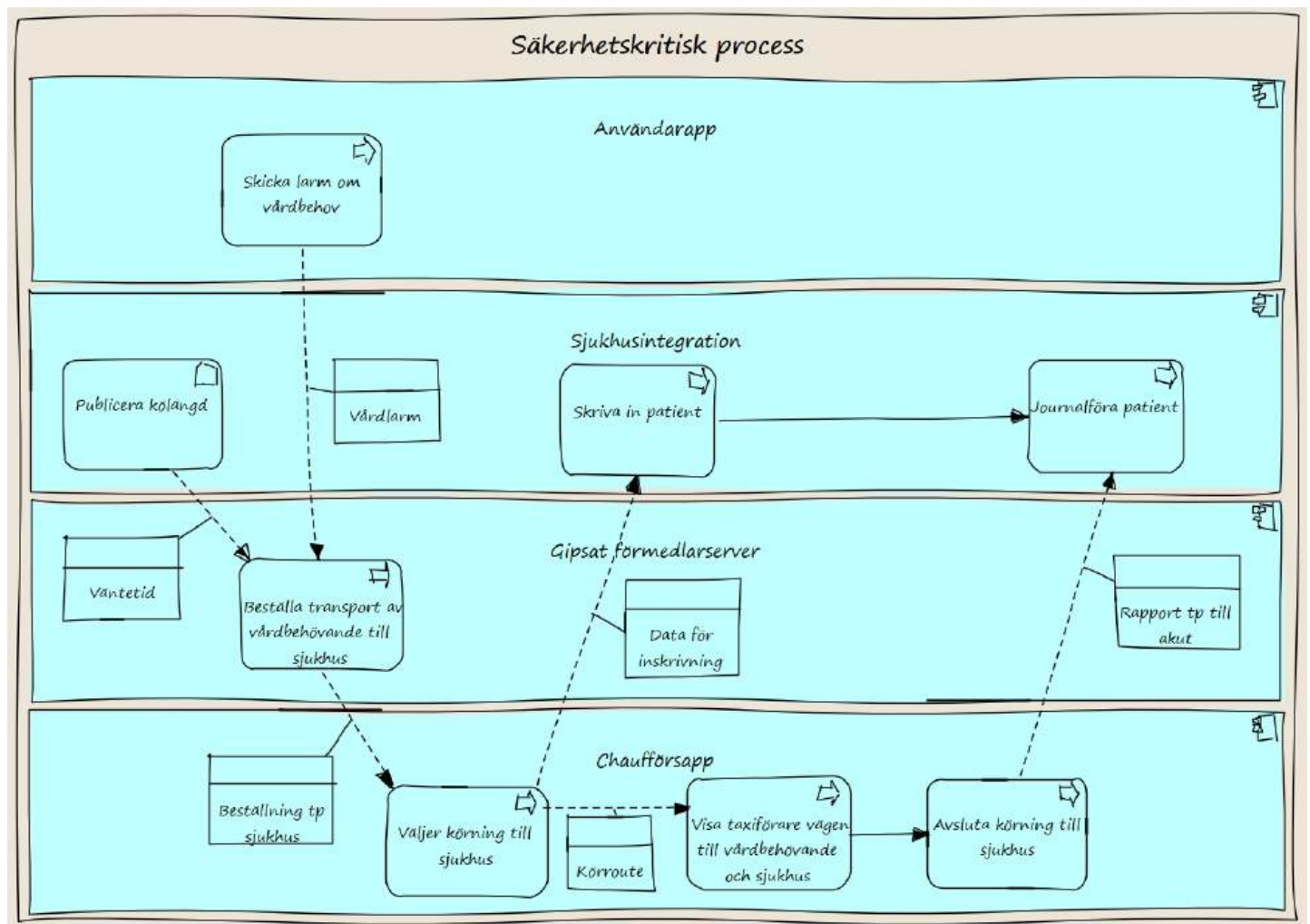
Gör en podd av underlaget. Podden ska verksamheten processen implementerar och berätta vad som händer när stegen inte fungerar. Deltagaren lyssnar och triggas långsamt tänkande "då skulle vi ju kunna ringa" eller "nej, det skulle inte hjälpa". och det är precis den bedömning hon ska göra i nästa steg:

3.5. Förberedelser till workshop

Skicka underlaget och podden några dagar i förväg. Varje deltagare sätter en vikt 1–5 per applikationsprocess. Motiveringen är det viktiga.

Sammanställ svaren före mötet. Där alla landat lika tar diskussionen två minuter. Där svaren spretar från 2 till 5 ligger antingen en okänd barriär eller en missuppfattning om vad steget gör, och det är där mötets tid ska läggas.

3.6 Workshopen, analysera förberedelserna och komma överens om resultat



Workshopen syfte är att synkronisera förberedelserna till säkerhetskritisk process. Agenda:

- 10 min. Gå igenom de enskildas resultat utan att diskutera, notera var det spretar.
- 20 min. Där rösterna spretar. Vad vet den som röstade lågt som de andra inte vet?
- 15 min. Processen, vilken är säkerhetsprocessen.

Resultatet är dels en tabell med allokerad vikt per applikationsprocess men framför allt är det den säkerhetskritiska processen.

- Tabell med viktade aktiviteter

+

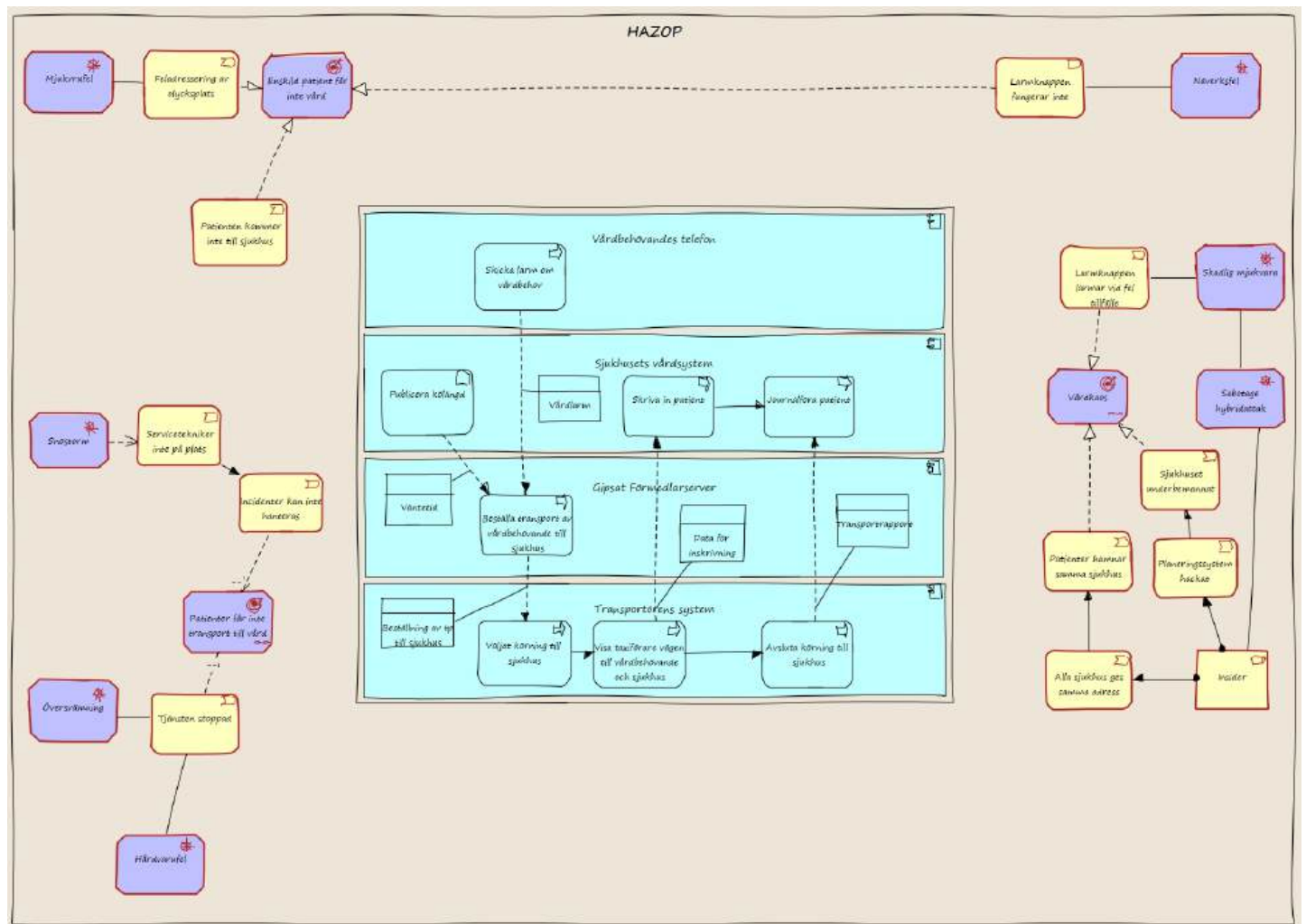
4. RISKANALYS AV FAROR INIFRÅN (HAZOP)

4.1. Riskanalys enligt HAZOP hittar faror och risker utifrån din organisations processer

HAZID tittade utifrån och frågade vad som kan hota tjänsten. HAZOP tittar inifrån och frågar vad som kan gå fel i arbetet. Olika riktning ger två olika sorters fynd. HAZOP hittar orsakerna till i HAZID funna outcomes . Men den hittar också nya outcomes, konsekvenser ingen såg utifrån.

HAZOP (Hazard and Operability Study) är en riskanalys utifrån processer och system. Riskanalysen enligt HAZOP hittar faror och hot inifrån. Här är HAZOP övergripande anpassat för cybersäkerhet.

4.2. Ta fram underlaget för riskanalys enligt HAZOP baserat på resultatet från HAZID

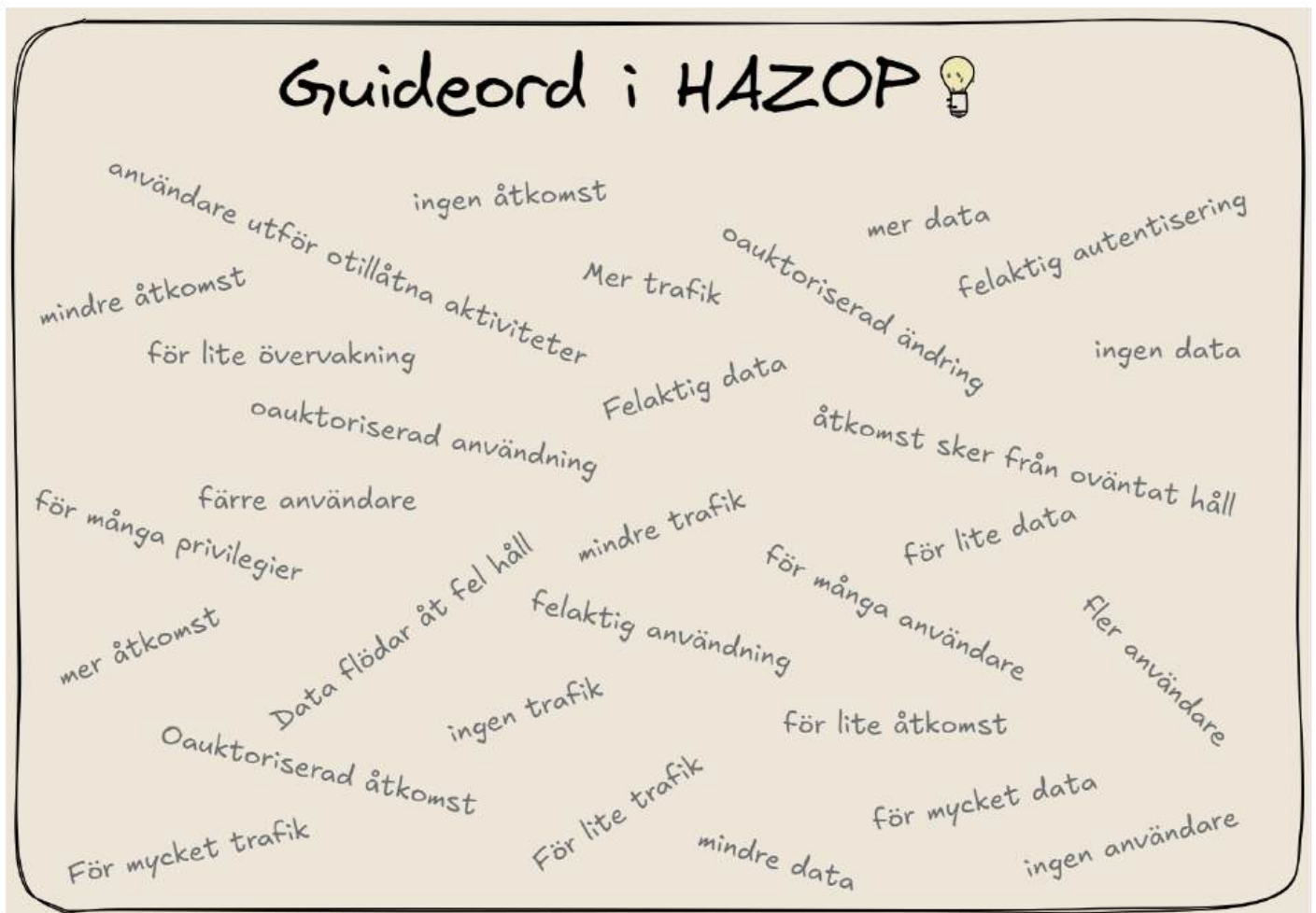


Du kan inte köra HAZOP på hela processen på en gång. Avgränsning till säkerhetskritisk process gjordes kapitel 3.

För Gipsat.nu går den från att den skadade trycker på larmknappen till att patienten är inskriven på sjukhuset. Den startar i den skadades mobiltelefon, går via Gipsats förmedlarserver ut till taxiförarnas telefoner, och slutar i sjukhusets vårdsystem.

Fyra systemägare delar kedjan. Det avgör hur analysen läggs upp, ingen av dem har det kompletta flödet men tillsammans ser dom helheten.

4.3. Guideord inom cybersäkerhet för riskanalys enligt HAZOP

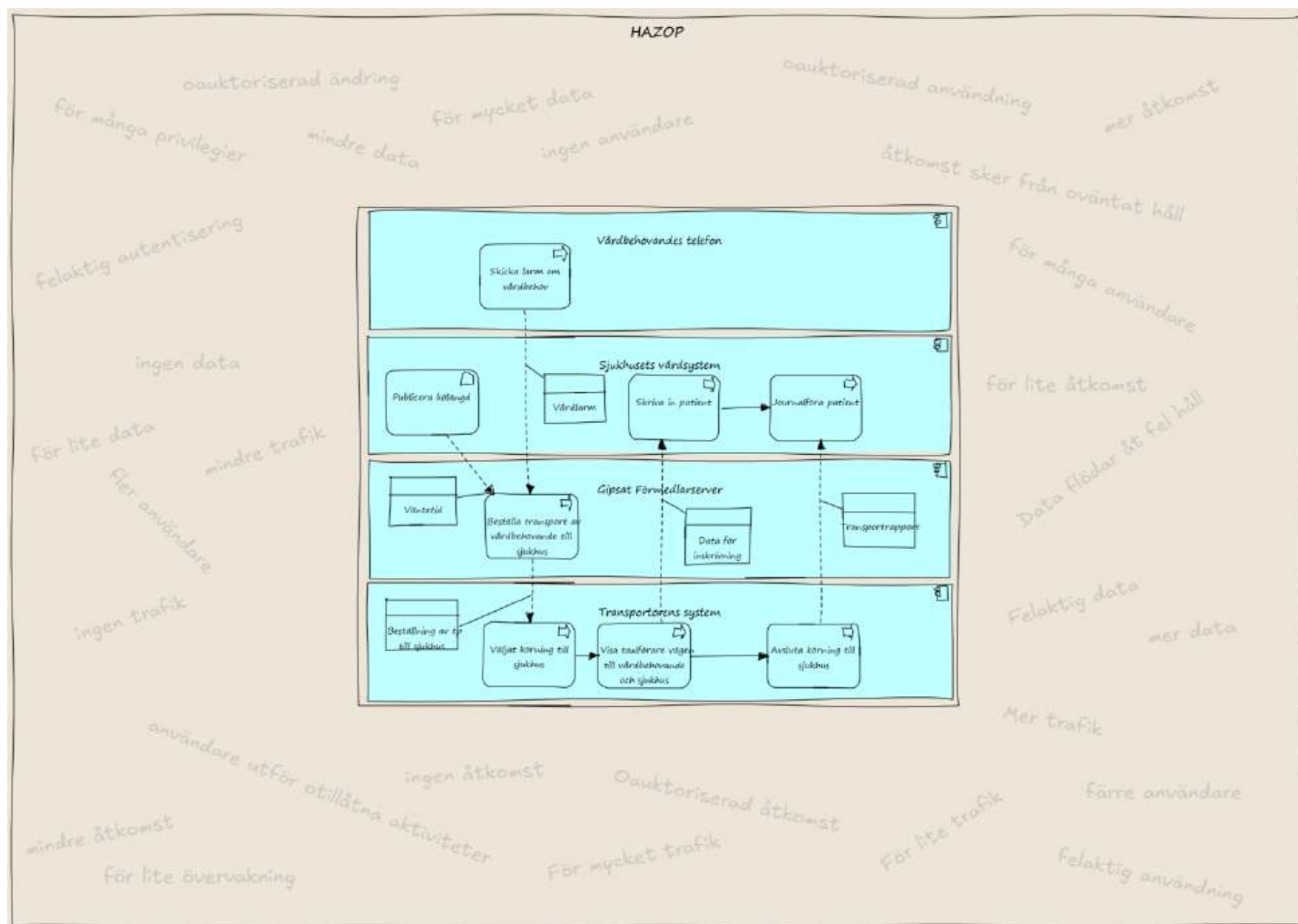


Applicera guideord för att hitta riskerna t ex :

- Mer trafik, data, åtkomst eller användare.
- Mindre trafik, data, åtkomst eller användare.
- Ingen trafik, data, åtkomst, eller användare.
- Omvänd: Data flödar åt fel håll, åtkomst sker från oväntat håll, användare utför otillåtna aktiviteter.
- Felaktig data, användning eller autentisering.
- För mycket trafik, data, användare, eller privilegier.

- För lite: För lite trafik, data, åtkomst eller övervakning.
- Oauktoriserad åtkomst, användning eller ändring.

4.4. Mall för HAZOP, informationsorienterade guideord och processen i mitten



Mallen har processen i mitten, precis som HAZID hade värdeerbjudandet. Informationsobjekten längs flödet, avvikelserna runt om, och de resultat de leder till ytterst.

Guideorden appliceras på informationen mellan aktiviteterna.

Håll analysen på logisk nivå. Systemägarna har riktiga system i huvudet och glider lätt in i teknik. Frågan är vad som lämnas över och vad mottagaren gör med det, inte hur överföringen sker. Protokoll och integrationer hör till systemriskanalysen.

4.5. AI i tar tre steg fram avvikelser

AI arbetar i samma tre steg dessa roller:

1. **AI-systemägare säkerhetsanalytiker** gör varsin HAZOP med HAZID stödord och annat underlag som grund.

2. **AI-säkerhetsanalytikern** sammanställer ai-intressenternas resultat till ett diagram.
3. **AI-angriparen** försöker hitta på djävulskap, varför inte ett hybridhot eller två.

Kombinatoriken är hårdare här än i HAZID. Sex avvikelsetyper med flera guideord vardera mot åtta processteg blir långt över hundra kombinationer. Vi låter återigen AI göra jobbet. Intressenterna är utbytta mot systemägare, de ser det inifrån vad som händer hos dem.

Det gör oenigheten i steg 2 särskilt värdefull. När två systemägare har olika bild av vad som lämnas över har ni hittat en lucka. En vanlig orsak till att kedjor går sönder, och den syns aldrig i en analys gjord av en part ensam.

En kontroll när sammanställningen är klar: hittade HAZOP några resultat som HAZID missade? Om inte har analysen körts för snävt. Det är inifrånperspektivet som ser det utifrånblicken inte kan se, transportrapporten som uteblir ser ut som en fungerande körning.

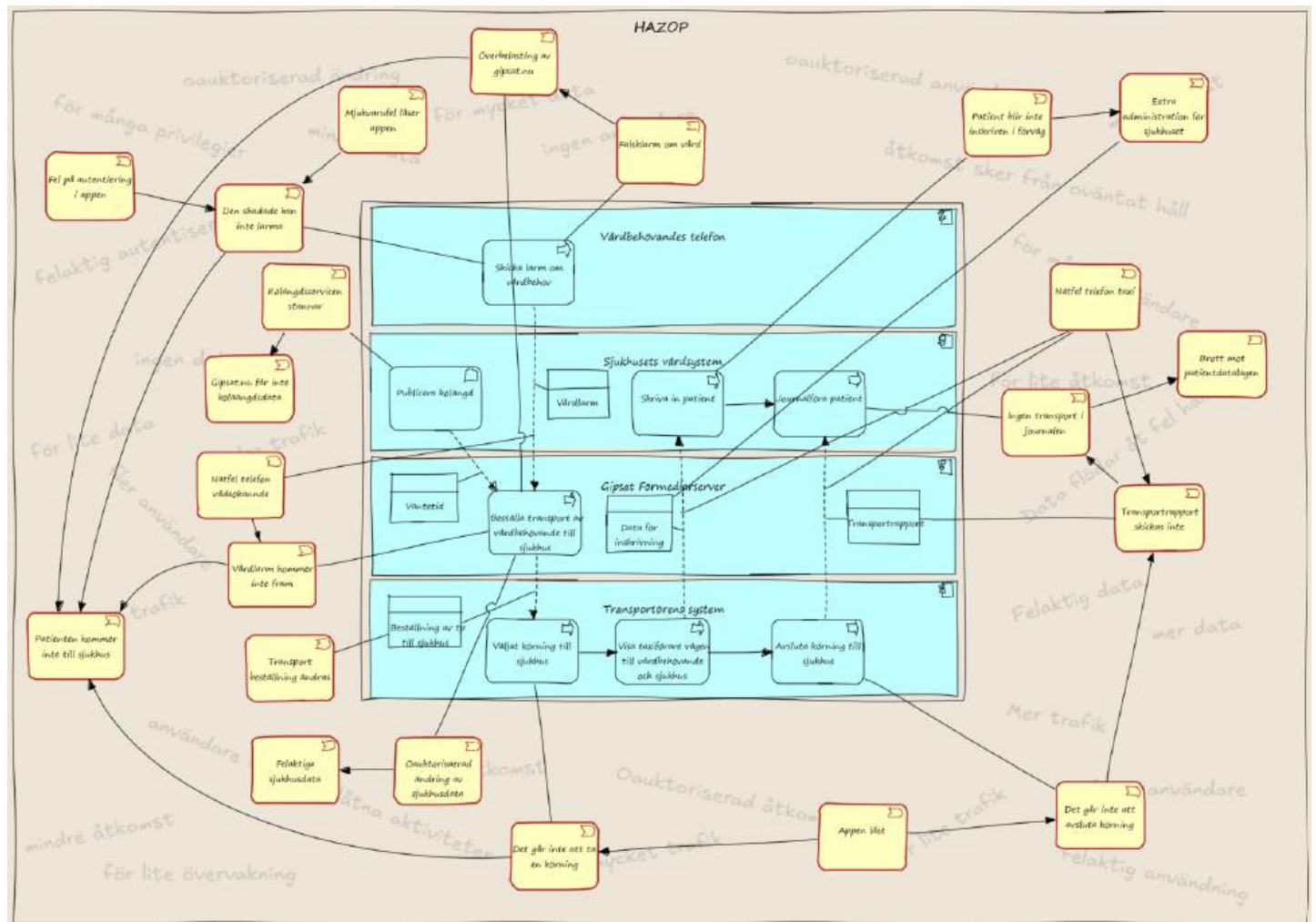
- **Prompt 1: Systemägarnas riskanalytiker gör HAZOP** +
- **Prompt 2: Chefsriskanalytikern sammanställer** +
- **Prompt 3: Angriparen angriper det sammanslagna** +
- **Podd** +

4.6. Deltagarnas förberedelser

Skicka ut diagrammet, listan över öppna frågor och en podd några dagar före workshopen.

Varje deltagare hänger sina notiser direkt på kedjorna, vid den punkt de gäller. Sätt deadline ett par dagar före mötet så att workshopledaren hinner sortera. En kedja med många notiser blir mötets tyngdpunkt. En kedja helt utan betyder antingen att den är uppenbart riktig eller att ingen orkat titta.

4.7. Workshop HAZOP



Samma upplägg som HAZID-workshopen: diagrammet på tavlan, enskild förberedelse, och mötet ägnat åt det AI inte kan avgöra. Agenda:

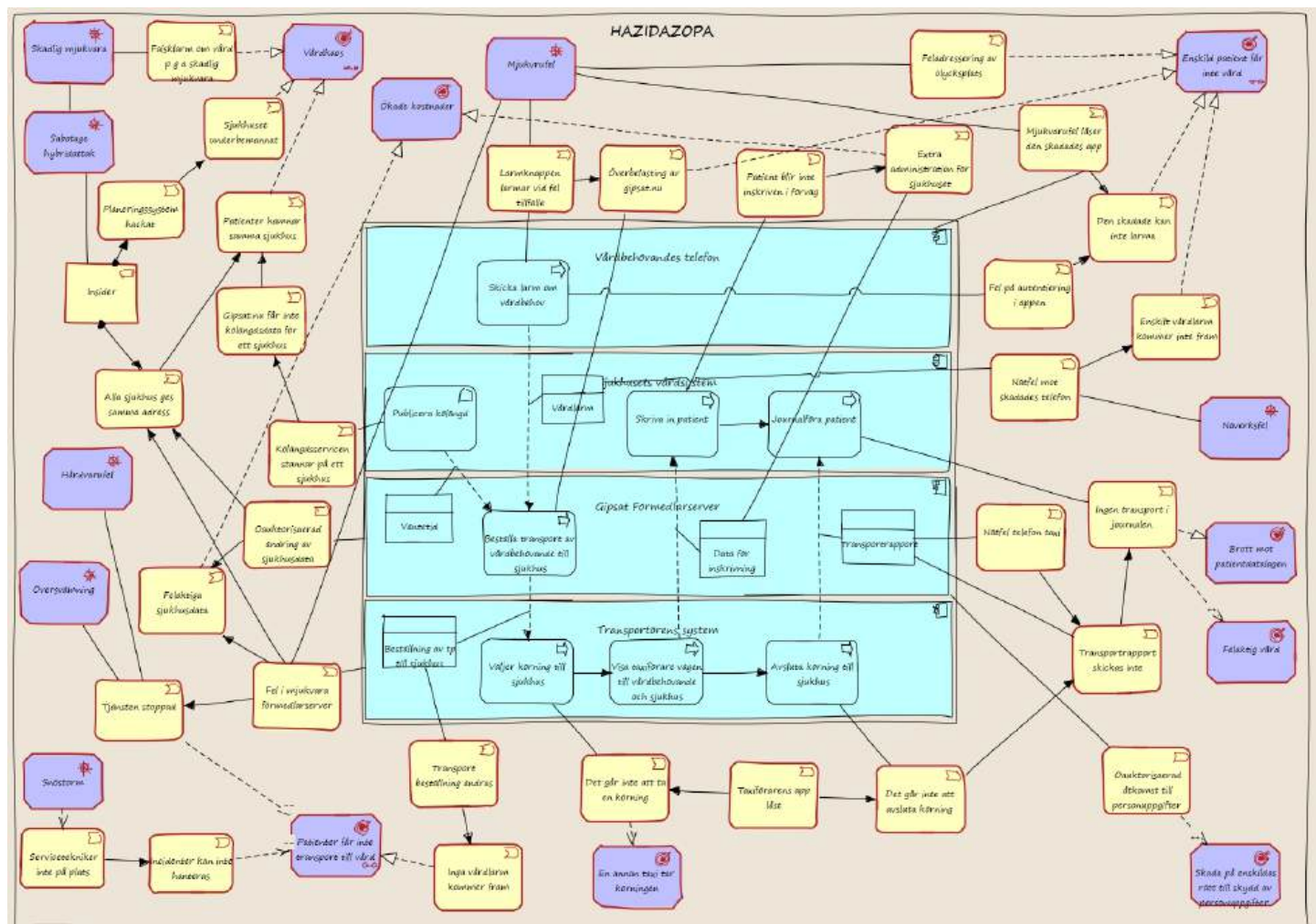
- 10 min. Genomgång av den sammanslagna bilden. Vad är hypotes, vad är verifierat.
- 45 min. Kedja för kedja med notiserna från förberedelsen. Vad har ni hängt upp, och vad gör vi med det?
- 10 min. Vad saknas, hittade vi något HAZID missade?
- 5 min. Sammanfattning och öppna frågor.

Efter workshpen formaliserar arkiyekten workshpresultatet i modellen.

HAZOP för gipsat.nu

5. SYNTES AV HAZID & HAZOP

5.1 Slå ihop blackboxtänket med processanalysen,



Skapa en syntes av HAZID och HAZOP. Lägg din HAZID utanför HAZOP. Lägg därefter in alla relationer mellan HAZOP och HAZID.

Efter detta analyseras resultatet med Intressenternas säkerhetskrav i åtanke. Leta efter händelser du missat och potentiella konsekvenser: Dataintrång, systemfel, förlust av affärsvärde, rykteskada.

Försök både att hitta konsekvensen hybridattacker från enskilda konsekvenser och enskilda konsekvenser av hybridattacker. Här gäller bredd i analysen.

- HAZOP för gipsat.nu

+

5.2 Single point of failure

En SPOF är något som flera kedjor beror på samtidigt. Den är svår att se i en enskild analys, eftersom varje kedja ser rimlig ut var för sig — det är först när de ligger bredvid varandra som det gemensamma träder fram.

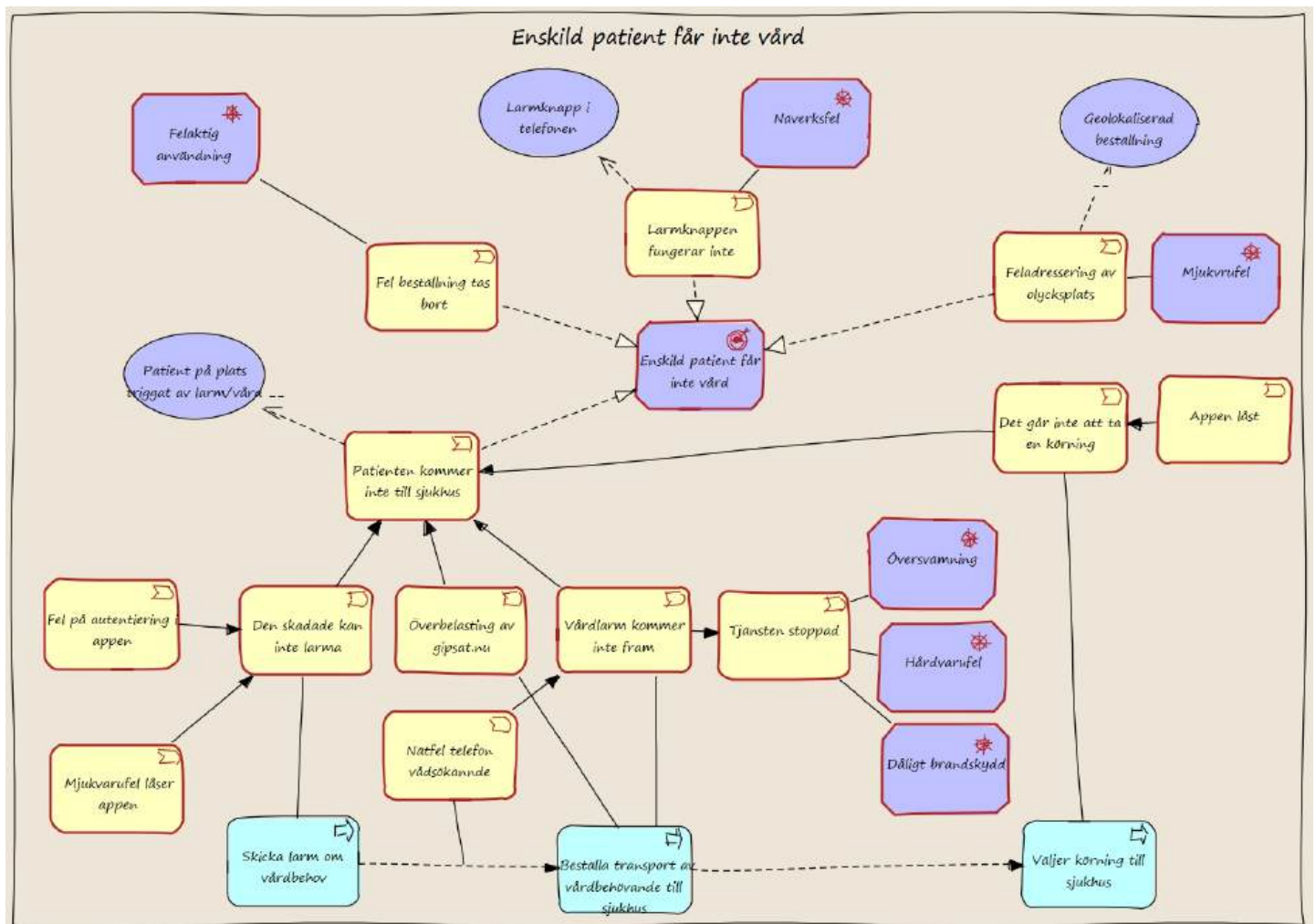
Fyra sorter att leta efter:

1. Gemensamt element. En farlig händelse eller avvikelse som förekommer i flera kedjor. Insidern i Gipsat-exemplet bidrar till två kedjor samtidigt, och det gör att två oberoende scenarier plötsligt har en gemensam startpunkt.
2. Gemensam leverantör. Flera led beror på samma part. För Gipsat äger transportören både körningsval och rapportering — faller den ut träffas både vårdkedjan och integritetskedjan.
3. Gemensam infrastruktur. Samma nätverk, samma molntjänst, samma identitetshantering. Redundans som ligger hos samma leverantör är ingen redundans.
4. Gemensam person. Den som är ensam om att kunna något. Semester och sjukdom räcker för att utlösa den.

Hur ni hittar dem. Gå igenom elementen i den sammanslagna bilden och räkna hur många kedjor var och ett förekommer i. Allt som finns i mer än en är en kandidat. Ställ sedan frågan baklänges: om det här fallerar, vilka kedjor rör sig samtidigt?

Varför det spelar roll i nästa steg. En SPOF gör att risker ni bedömt som oberoende inträffar tillsammans. Det ändrar inte den enskilda risknivån, men det ändrar sannolikheten för att flera inträffar samtidigt — och det är precis vad ett hybridhot är. Vårdkaos är tre förlopp som ser oberoende ut och delar angripare.

5.3 Beskriv faror, konsekver och risker



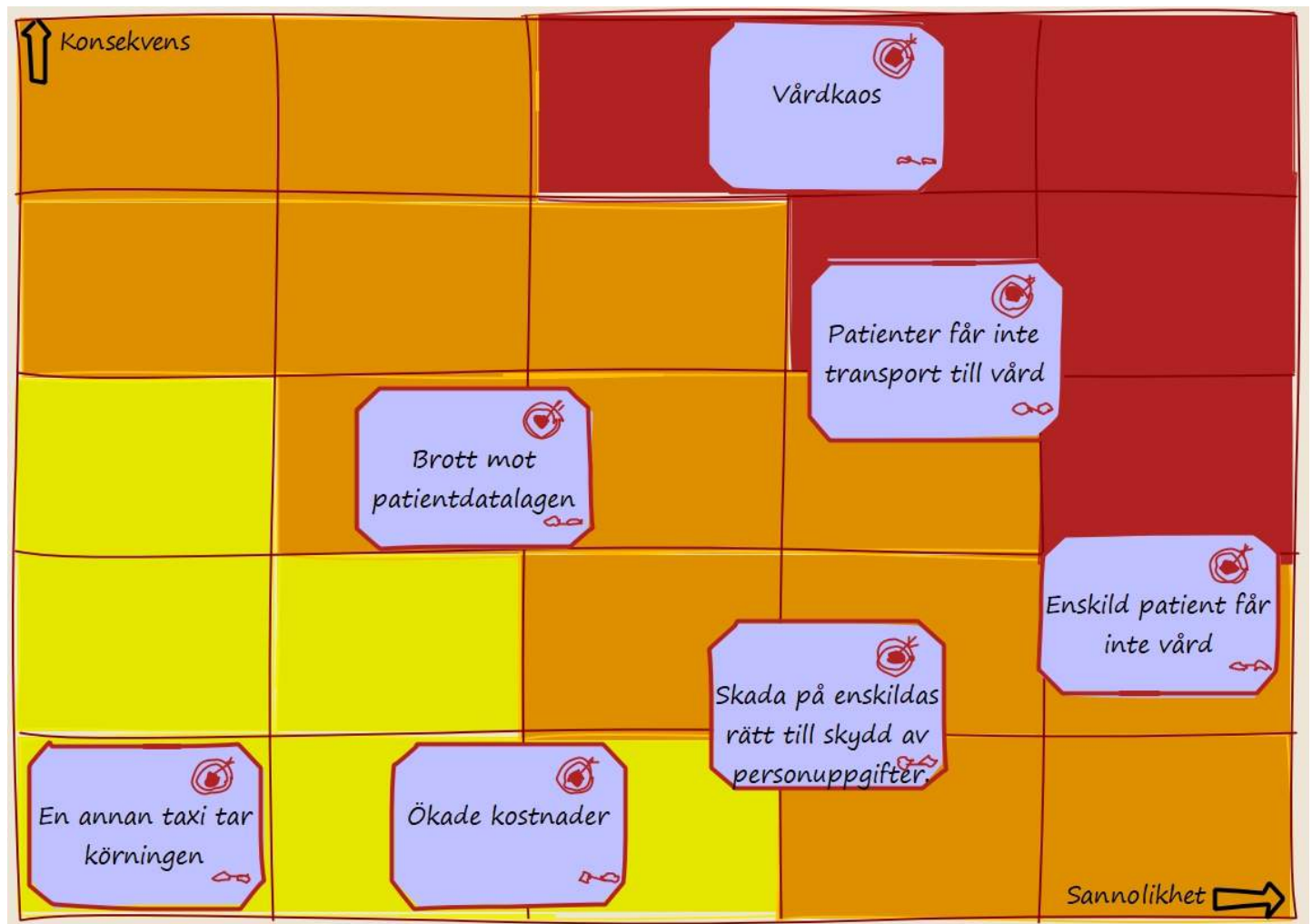
Sätt nu den enskilda konsekvensen i centrum. Utifrån den placerar du in de farliga händelserna som kan leda till den. Analysera konsekvensen, diskutera och dokumentera:

- Möjliga konsekvenser: Dataintrång, systemfel, förlust av affärsvärde, rykteskada.
- Sannolikhet: Hur troligt är det att avvikelserna inträffar?
- Se till att berörda tjänster finns med.
- Analysera befintliga kontroller och hur dessa påverkar och påverkas av olika guideord.
Exempel på guideord anpassade för cybersäkerhet.

Befintliga skydd noteras, men räknas inte in i riskanalysen här, det kommer vid säkerhetsbeviset. Kommer det upp att något redan finns på plats, skriv upp det vid risken, det används i riskbehandlingen. Här bedöms risken som den är, annars går det inte att senare visa vad åtgärderna gav.

6. FASTSTÄLLA RISKNIVÅ OCH PRIORITERA BLAND RISKERNA

6.1. Bedöm sannolikhet för och konsekvens i en riskmatris



Riskerna har identifierats med händelsekedjor samt de resultat riskerna leder till. Nu ska du för varje risk bedöma konsekvenserna av risken samt sannolikheten för att den inträffar. Detta gör du traditionellt genom att bedöma riskernas sannolikhet och konsekvens i en riskmatris.

Riskmatrisen är det första steget i att fastställa risknivån och en bra grafisk ingång. Men riskmatrisen räcker inte för att prioritera. Tio risker kan hamna i samma ruta, och matrisen säger ingenting om vilken av dem som betyder mest för just er verksamhet. Nästa avsnitt visar hur du löser detta.

6.2. Prioritera riskerna med WPRF

Weighted Prioritised Risk First (WPRF) rangordnar och prioriterar riskerna. Genom att bedöma varje risk från 1–5 i fyra konsekvensområden, och sedan väga ihop dem, prioriterar WPRF mellan riskerna. Tänk på att siffrorna är ett verktyg för prioritering, det innebär att om du ger alla risker en 5:a, har du i praktiken inte gjort någon prioritering alls. Metoden och hur resultatet används beskrivs i detalj på sidan om Weighted Prioritised Risk First. Nedan ser du resultatet för gipsat.nu

6.3 Riskbeslutspunkt 1 och vägen vidare

Det här var den första av två WPRF-körningar. Här prioriterades risker på verksamhetsnivå, innan ni vet något om tekniken. Den andra görs i systemriskanalysen, mot den funktionella och logiska arkitekturen.

Riskbeslutspunkt 1. Räcker underlaget för att avgöra vad som krävs för att få ner riskerna till acceptabel nivå? Om inte görs en ny iteration – med ändrad omfattning, annan expertis eller kompletterat underlag.

För Gipsat var svaret nej första gången. Integritetskedjan saknades, och patientuppgifternas väg genom transportledet hade inte följts. Efter en kompletterande genomgång tillkom risken som nu ligger trea.

Här bekräftas också viktningen från kapitel 2. Den byggde på HAZID; nu har ni hela analysen.

Risklistan är inte målet. Den går in i policyarbetet, där varje tänkbar säkerhetsstrategi ställs mot de risker den täcker. För Gipsat visar det sig att safety by design och rimlighetskontroll av resultat tillsammans adresserar de tre översta riskerna, medan skydd mot skadlig kod bara når en av dem – men till en bråkdel av insatsen.

En strategi som tar bort en femtedel av tre risker slår en som tar bort hälften av en, och det syns inte när man arbetar risk för risk. Hur strategierna väljs beskrivs i policyartikeln.

FAQ RISKANALYS: PRELIMINÄR RISKANALYS OCH VÄGEN TILL SÄKERHETSKRAV

- | | |
|--|---|
| <u>1. Varför räknas både HAZID och HAZOP som preliminär riskanalys hos Ension?</u> | + |
| <u>2. Vad är målet med denna inledande screening?</u> | + |
| <u>3. Hur leder den preliminära analysen vidare till "Riskanalys System"?</u> | + |
| <u>4. Vad innebär en "allriskansats" i detta skede?</u> | + |
| <u>5. Varför är det viktigt att hitta SPOF (Single Points of Failure) redan nu?</u> | + |
| <u>6. Hur skapas säkerhetskraven utifrån dessa analyser?</u> | + |
| <u>7. Kan riskanalysen motivera att vi inte använder MFA?</u> | + |
| <u>8. Vad händer om vi hoppar över den preliminära analysen och går direkt på tekniska krav?</u> | + |
| <u>9. Hur säkerställer Ension att kraven faktiskt uppfyller lagen?</u> | + |
| <u>10. Vilket ansvar har ledningen i detta flöde?</u> | + |

Den här siden är under utveckling, den blir sakta bättre . Kom gärna med åsikter och frågor.

U L F D E L L B O R G

