Universitetet i Stavanger

KANDIDAT

5408

PRØVE

SAM505 1 Risiko og samfunnssikkerhet

Emnekode	SAM505
Vurderingsform	Skriftlig eksamen
Starttid	12.12.2023 08:00
Sluttid	12.12.2023 13:00
Sensurfrist	02.01.2024 22:59
PDF opprettet	28.08.2024 12:18

Introduksjon

Oppgave	Tittel	Oppgavetype
i	Forside	Informasjon eller ressurser
i	Grading scale	Informasjon eller ressurser
i	Informasjon om eksamen	Informasjon eller ressurser

Seksjon A

Oppgave	Tittel	Oppgavetype
1	Organizational accidents	Langsvar
2	Risk Governance	Langsvar

Seksjon B

Oppgave	Tittel	Oppgavetype
3	Risk,safety og security	Langsvar
4	Organizational accidents and Risk Governance	Langsvar

Seksjon A

Oppgavesettet består av to seksjoner, seksjon A og B. Kandidaten skal velge en av seksjonene, og besvare begge oppgaver i valgt seksjon.

1 Organizational accidents

Hva menes med organisatoriske ulykker, og hva menes med «forsvar»? Gjør deretter rede for begrepene «aktive feil» og «latente betingelser».

Skriv ditt svar her

Organisatoriske ulykker og High Reliability Organizations - James Reason

Med organisatoriske ulykker mener vi ulykker som oppstår i komplekse, ofte store (tekniske) systemer hvor ulike systemer, delsystemer, subsystemer har ulike koblinger til hverandre og er avhengige av hverandre for å fungere. Det er ikke så ofte at organisatoriske ulykker oppstår, men når de først oppstår er det gjerne en situasjon med stor kompleksitet og stort skadeomfang (f.eks. feil i et atomkraftverk), fordi at disse omfattende systemene er så komplekse. Disse risikoene og systemene er gjerne produsert i "den moderne verden" og/eller "risikosamfunnet", da systemene kjennetegnes av stor teknologisk kompleksitet (mer om dette i tilhørende temaer).

Tillit, robusthet og resiliens

James Reason mener at organisatoriske ulykker kan unngås ved å skape organisasjoner og systemer som har en god organisasjonskultur og god sikkerhetskultur, som videre bidrar til robuste og resiliente organisasjoner og systemer. Robuste systemer hvor feil oppdages tidlig kan inkorporeres ved at de ansatte som både utvikler og arbeider i systemene har ulike bakgrunner som gjør at de kan bidra med ulike synspunkt og ulik fagkunnskap, noe som gjør at de kan kommunisere, diskutere og rådføre seg med hverandre, samtidig som at de har ulike utgangspunkt for å oppdage og avdekke feil eller trusler. Feil, trusler og usikkerheter som oppdages bør kunne reduseres og arbeides med på det nivået

de oppdager det på, hvor organisasjonen har tillit til sine medarbeidere, hvor problemer kan løses på alle nivåer (desentralisert styring).

Organisasjonskultur og sikkerhetskultur

Organisasjonskultur og sikkerhetskultur går veldig inn i hverandre, og man må ha en god organisasjonskultur for å skape en god sikkerhetskultur. God organisasjonskultur og sikkerhetskultur kjennetegnes ved at alle har en felles forståelse av hva organisasjonen står inne for og representerer når det kommer til verdier og holdninger, og videre at alle er enige og inneforstått med, samt støtter de sikkerhets-målene organisasjonen jobber og står inne for. God organisasjonskultur skaper ved at man har tillit til hverandre (tørr å melde i fra om feil), er åpne og ærlige med hverandre dersom man oppdager feil eller usikkerheter (rapporterende kultur, det blir sett på som positivt å melde fra om avvik), det er en reflekterende og lærende organisasjon hvor man tar imot ny kunnskap på en positiv måte, og ønsker å lære nye ting relatert til systemene og organisasjonene man jobber med. Det er også viktig å lære av tidligere feil eller hendelser for å kunne skape robuste systemer, og implementere tiltak som takler en eventuell slik hendelse eller feil igjen.

Forsvar i dybden - Swiss cheese modellen

Knyttet til organisatoriske ulykker og høypålitelige organisasjoner er det introdusert en teori om forsvar-i-dybden, også kalt for "Swiss cheese modellen". Dette er en modell som fremstiller forskjellige lag med osteskiver på rekke, hvor hver osteskive skal illustrere ulike barrierer og forsvar i en organisasjon. En del av barrierene kan være knyttet til organisatorisk ansvar (som står på alle), mens den andre delen av barrierer kan være knyttet til egenansvar (ansvaret du som enkeltperson har for å ivareta sikkerheten).

Med forsvar mener vi tiltak og sikkerhetsstyring som forsøker å gjøre et system så robust og resilient som mulig. Hver enkelt barriere (forsvar) har forskjellige

fokusområder og sikkerhetsområder (beskyttelse på ulike nivåer), slik at dersom ett forsvar eller en barriere svikter, vil et annet og overlappende barriere forhåpentligvis fange opp risikoen, usikkerheten, feilen eller trusselen. Vi skiller mellom harde forsvar og myke forsvar:

- Harde forsvar er gjerne fysiske sikkerheter og sikkerhetssystemer, lås, koder, nøkler, alarmer osv.
- Myke forsvar er gjerne organisasjonskultur, sikkerhetskultur, kursing, opplæring, debriefing osv.

Dersom vi skal prøve å sette infrastruktur og organisering av et fengsel i en forsvar-i-dybden sammenheng, ville dette vært relevante barrierer og forsvar: Harde forsvar kunne bestått av sikkerhetskultur, sikkerhetskurs i selvforsvar, kursing og opplæring på hvordan å håndtere utfordrende situasjoner og utagerende innsatte. Myke forsvar kunne bestått av uniform som inneholder alarm og samband for å melde om hendelser, egne nøkkel sett og nøkkelkort med individuelle koder.

Alle disse forsvarene og barrierene symboliserer egne "osteskiver", og latente feil symboliserer "svakhetene" med de ulike barrierene, som er punkter hvor en barriere sannsynligvis vil svikte. Barrierene skal etter beste evne overlappe for hverandre; dersom man ikke klarer å deeskalere en situasjon mellom innsatte, har man alarm og samband å tilkalle hjelp med, eller man har kurs i selvforsvar. Dersom man blir frastjålet eller minster et nøkkelsett, vil barrierene med dører som også trenger nøkkelkort og individuelle koder føre til at innsatte ikke klarer å komme seg langt. Det er altså overlappende barrierer som fanger opp uønskede hendelser eller feil, og klarer å stabilisere situasjonen uten at det blir en uønsket hendelse, og som kan kompensere for de latente feilene ved barrierene.

Aktive feil kan være at mennesker legger fra seg nøkkel settet, eller for eksempel glemmer å ta på seg sikkerhets-alarm når man går ut på avdeling. Disse aktive feilene kan fanges opp og håndteres ved at som nevnt tidigere ved at

man ikke kommer seg så langt med bare nøkler og uten nøkkelkort, eller at man har samband eller forsvarskurs til å melde ifra om man skulle trenge hjelp.

Dersom alle disse aktive feilene og latente betingelsene (en feil fører direkte til en annen feil) skulle oppstått samtidig, for eksempel at; en betjent glemmer både alarm samband, som fører til at innsatte skaper en gisselsituasjon, hvor de overkjører alle teknologiske systemer og sikkerhetssystemer, truer ledelsen med å gjøre noe alvorlig dersom de ikke slippes ut i det fri, oppstår det mange systemsvikt og alle barrierer forsvinner på en gang. Slike latente betingelser som er situasjoner hvor det er bakenforliggende og utløsende årsaker som fører til at et system svikter, skjer gjerne når alle barrierer svikter på en og samme gang. Da kan det oppstå katastrofale hendelser (som f.eks. et stort opprør i et fengsel hvor innsatte tar kontroll og styringen i fengselet, låser opp alle dører og overstyrer sentralsystemet slik at innsatte kan flykte).

I høypålitelige systemer med forsvar i dybden skal i utgangspunktet slike situasjoner og organisasjons-ulykker/hendelser ikke oppstå, da barrierene skal kompensere for hverandre. Men worst-case kan det bli katastrofale ulykker og hendelser hvor resiliens og robustheten i organisasjonen ikke er godt nok, og farer og trusler skjærer gjennom alle barrierer.

Supplerende temaer og andre kommentarer

Motstridende syn på risikostyring - Charles Perrow og Normal Accidents:

Charles Perrow har et helt motstridende syn på risikostyring. Perrow mener at ulykker er uunngåelige, og at systemer er delt opp i deler, enheter, subsystemer og systemer som på et eller annet punkt vil skape en kombinasjon av risiko og usikkerhet som vil slå seg sammen til en uforutsett hendelse og føre til en organisasjonsulykke (Perrow skiller mellom hendelse og ulykke, ut ifra hvor i systemet det oppstår, og om det er noe systemet har kapasitet til å håndtere). Ettersom Perrow mener at disse ulykkene ikke kan unngås, omtaler han de som

"normale ulykker". Perrow mener at vi ikke vil klare å forebygge alle risikoer og hendelsene, fordi at de i kombinasjoner med hverandre utgjør uendelige kombinasjoner av risikoer og usikkerheter, og at det på et eller annet tidspunkt vil oppstå en kombinasjon av hendelser vi ikke har et forsvar mot. Perrow mener også at systemulykker gjerne utvikles ut i fra forskjellige forhold og tid, men at det gjerne er kombinasjonen av lineære, komplekse, tette og løse koplinger som fører til at ulykker skjer.

Perrow kritiserer også Reason sin teori om HRO-er, og mener at systemfeil uansett vil oppstå. Perrow har ikke tiltro til organisasjonskultur og sikkerhetskultur slik som Reason framstiller at det er mulig å bruke i forebygging av organisatoriske ulykker. Perrow mener at delegering av håndtering og ansvar vil ikke fungere i praksis, hvertfall ikke under krisesituasjoner fordi da vil styringen gjerne gå opp til ledelsen igjen. Han mener også at mange organisatoriske ulykker bygger seg opp over tid og vil trolig ikke skje mens de som leder nå er ansvarlige, noe som fører til at de prioriterer styring med best kostnadseffektivitet og alternativer som gir størst uttelling.

Risikosamfunnet - Ulrich Beck:

Organisatoriske ulykker (og NA) kan kobles opp mot "risikosamfunnet" og den moderne verden som står av komplekse systemer som inneholder mye usikkerhet, og derfor bidrar med utallige usikkerheter og risikoer. Vi lever i en kompleks og globalisert verden, og ifølge Beck skaper risikosamfunnet utfordringer og teknologiske systemer med usikkerhet og risikoer vi selv sliter med å håndtere, og som slår tilbake på oss selv gjennom ulykker.

Risikoer kan dog ha både positive og negative utfall, og vi kan lære noe av både positive og negative konsekvenser og utfall av risikoer. Det er på grunn av folks villighet og evne til å ta risiko at samfunnet går fremover, og at vi oppdager nye ting og skaffer oss ny kunnskap og kompetanse.

Safety og security:

Knyttet til risikoer og usikkerheter i organisatoriske ulykker kan man også skille mellom safety (ikke-planalgte hendelser) og security (intenderte (ofte ondartede) uønskede hendelser, og disse kan påvirke hverandre. En person som jobber som betjent i fengselet kan i teorien være en del av organisasjonen og systemet, men ønske å påføre systemet skade ved å utføre en security-handling. En ansatt i fengselet kan i teorien ha så god kjennskap til barrierer og sikkerhetssystemet at hen vet hvordan hen skal overstyre systemet og utføre en security-handling. Safety-situasjoner som naturkatastrofer kan også i teorien skape så store skader på f.eks. en oljeplattform som fører til store oljeutslipp og store miljøkonsekvenser. Black swans kan også være hendelser som ingen hadde sett komme, som skaper usikkerhet og konsekvenser i organisasjoner.

Tillit, refleksivitet og odontologisk usikkerhet - Anthony Giddens:

Organisatoriske ulykker kan også knyttes til Anthony Giddens syn på risiko, og at ekspertkunnskap og tillit til ekspertsystemene skaper en ontologisk usikkerhet. Dersom ekspertsystemer kollapser og organisatoriske ulykker oppstår, fører det til en ontologisk usikkerhet som videre kan bidra til å skape tvil til ekspertsystemene, samtidig som vi mister tillit til ekspertsystemene og organisasjonene som står ansvarlige for risikohåndteringen. Det kan også føre til usikkerhet og påvirke vårt syn på risiko.

Ord: 1650

2 Risk Governance

I Renn (2008) blir det skilt mellom ulike typer risikosituasjoner (risikoproblemer). Dette skillet blir bestemt av graden av kompleksitet, usikkerhet og tvetydighet. Redegjør for hvordan Renn anvender disse begrepene (kompleksitet, usikkerhet og tvetydighet) i en systematisk analyse av risiko. Hvilken betydning har resultatet av en slik analyse for risikostyringsprosessen (Risk Governance)?

Skriv ditt svar her

Risk Governance Framework (IRGC-modellen)

Rammeverket

Rammeverket og modellen har en "dual nature", da den inneholder både teknisk-ønokomiske, psykologiske og sosiale perspektiver/hensyn til risiko (det vil si ulike modeller for risiko, regning av risiko, styring av risiko, samtidig som den tar hensyn til folks og samfunnets oppfatning av risiko og risikopersepsjon). Modellen inneholder ulike perspektiver knyttet til risiko og risikostyring, som forteller oss noe om hvordan vi kan tolke risikoene, styre og håndtere risikoene, og iverksette aktuelle beslutnings metoder- og tiltak for å opprettholde sikkerheten i samfunnet på best mulig vis. Risiko forklares som usikkerhet knyttet til hva hendelser og konsekvenser av risikoer kan være, og som setter noe vi mennesker verdsetter i fare.

Modellen har stort fokus på involvering av "stakeholders". Målet med risikostyringen er å komme fram til om risikoene er ikke-tolerable, tolerable eller akseptable. Dersom risikoen er tolerabel, ønsker vi å få nytte av den verdien og gevinsten det ligger i å ha risikoen til stede, og vi er derfor villige til å innføre ulike tiltak som gjør at risikoen ligger på et tolerabelt nivå. Dersom risikoen er akseptabel, synes vi det er greit at den er der og vi føler ikke behov for å endre den eller gjøre noe med den, det er risikoer vi fint klarer å leve med.

Gjennomgang av modellen

Risk governance modellen består av to såkalte sfærer; "management sphere" og "assessment sphere". Disse kan oversettes til ledelsessfæren (implementering av tiltak og styring av sikkerhet) og styingssfæren (innhenting av risikoinformasjon).

1. Førvurdering

Førvurderingen er starten av prosessen hvor vi velger oss ut risikoer vi ønsker å arbeide med og ta med videre, dette gjør vi gjennom prosesser som "screening", "framing" og vi leter etter risikoer som kan utgjøre farer eller usikkerheter. Her velger vi fokusområder og risikoer som vi ønsker å jobbe nærmere med i neste steg (risikovurderingen).

2. Risikovurdering

Vi tar med oss de risikoene som er valgt ut fra førvurderingen, og skal i denne prosessen skaffe oss enda mer informasjon om de utvalgte risikoene, og vurdere risikoene ytterligere.

Risikovurdering inneholder to ulike steg: gjennom det første steget tar vi hensyn til den teknisk-økonomiske som gjerne setter tall på og måler risikoer ut i fra modeller og teorier, mens det andre steget setter fokus på folks oppfatninger, samfunnets oppfatninger av risikoene og hvordan f.eks. det kan påvirket omdømmet.

I denne delen av prosessen møter vi også kunnskapsutfordringer knyttet til risikoene, det handler om å plassere risikoene som enkle, komplekse, usikre eller tvetydige. Basert på kompleksiteten, usikkerheten og tvetydigheten av risikoene vil det variere til hvilken grad det blir nødvendig å inkludere ekspertkunnskap og stakeholders. Dette er en viktig del av prosessen og

stakeholder-involvement, og jeg utdyper denne kunnskapsutfordringen nedenfor i oppgaven.

3. Aksept- og toleransevurdering

I denne delen tar vi igjen med oss risikoene vi har arbeidet med og skaffet oss informasjon om i de tidligere punktene, og grad av involvering av stakeholders vil følge med oss til denne prosessen. Dersom vi føler at vi har nok informasjon og en god forståelse av risikoene (ved enkle eller til dels komplekse risikoer) trenger de ikke bli med videre til punkt fire som omhandler risikostyring, men dersom risikoene er usikre og tvetydige føler stakeholders og ekspertene (eventuelt interessenter og samfunnet generelt) gjerne med.

Dette er den største og viktigste delen av prosessen. Den omfatter både risikovurdering og risikoevaluering (aleatorisk og epistemisk usikkerhet). Dette er to prosesser som bør gjennomføres parallelt siden de går veldig inn i hverandre. Risikovurdering kan f.eks. framstilles ved å bruke risiko matrise (de skal ikke brukes i praksis, men de tydeliggjør hvor risikoene i utgangspunktet er plassert; rød, gul eller grønn). I faktisk risikostyring vil de være for lite konkrete, men i modellen er de brukt som et eksempel. Gjennom risikoevalueringen må vi plassere risikoene innenfor kategoriene; ikke-akseptable, tolerable og akseptable.

Gjennom risikovurderingene og risikoevalueringen har vi skapt oss en (forhåpentligvis) god forståelse over risikoene (kanskje ved hjelp av stakeholder involvement). Det neste steget i prosessen avhenger av hvordan vi har kategorisert risikoene (tolerable, ikke-tolerable og tolerable).

4. Risikostyring

Når vi har bestemt oss for om vi synes at risikoene er akseptable, tolerable eller ikke-akseptable, må vi velge styringsstrategi og tiltak ut i fra hva vi ønsker å gjøre med de gjeldende risikoene. Vi kan bruke ulike metoder og modeller for å styrke

vår beslutningstaking som kost-nytte/kost-effektivitets analyser, for videre å bestemme oss for tiltak og risikostyringsstrategier.

Risikostyringen vil avhenge av kompleksiteten og usikkerheten knyttet til risikoen, hvor mange den påvirker og hvor alvorlig den er (om vi f.eks. må ta i bruk føre-var-prinsippet), og vi velger gjennom ulike styringsalternativ ut i fra om vi ønsker å gjøre noe med risikoen, la den være som den er, overføre den til noen andre eller fjerne den totalt.

I risk governance er det ikke opp til de som har gjort risikovurderingene og beslutte om tiltak skal iverksettes eller ikke, det er opp til myndighetene å bestemme. Eksperter, fagfolk og de som arbeider med risikoene har bare som oppgave å presentere de ulike risikoene, konsekvensene, usikkerhetene og sannsynlighetene knyttet til de, og presentere hvilke alternative håndterings-alternativ eller beslutnings-tiltak som kan være relevante.

Kommunikasjon

Kommunikasjon inngår i alle disse prosessene, og prosessen trenger kontinuerlig kommunikasjon mellom alle deltakere for å fungere optimalt. IRGC-modellen er en prosess hvor man gjerne kan bevege seg fram og tilbake mellom stegene, og kommunikasjon er derfor viktig. Ettersom modellen også inkluderer stakeholders og interessenter, vil hvordan man kommuniserer og samarbeider med deltakerne gjennom prosessen være veldig viktig.

Desto mer informert både stakeholders, interessenter og befolkningen er, desto mer kjennskap får vi til risiko, noe som også bidrar til å skape forståelse og kanskje en viss form for "trygghet". Det å kommunisere både hva man vet og hva man ikke vet, er viktig. Det bidrar til at befolkningen og interessenter føler seg inkludert i prosessen, og oppdatert på situasjonen. Det gjør det også enklere for alle å forholde seg til risikoen, og også ta gode beslutninger i relasjon til risiko og usikkerhet.

Risikokommunikasjon påvirker vår risikopersepsjon, og dersom vi føler oss inkluderte i prosessen har vi også gjerne større forståelse hvorfor myndighetene må opprette ulike tiltak (som under covid-19), og det vil også skape tillit til myndighetene. Igjen bidrar dette til et samfunn som forholder seg til tiltak og reguleringer, som også kan bidra til resiliens og robusthet i et samfunn (man opplever mindre smitte fordi innbyggerne følger tiltakene, fordi de har tillit til myndighetene, og mindre smitte gjenspeiler kanskje et mer robust og resilient samfunn).

Stakeholder invovlement

Det er når vi kommer til risikovurderingen i modellen, at punktet knyttet til kunnskapsutfordringene oppstår. Ut ifra risikoens grad av usikkerhet, kompleksitet eller tvetydighet, må vi vurdere hvor mye kunnskapsinnhenting og stakeholder-involvement som trengs for å forstå risikoen og dermed kunne analysere den riktig for så å komme fram til riktige risikostyringsstrategier eller beslutninger for å håndtere risikoen.

- *Enkle risikoer* - Beslutninger kan gjøres på et lavt nivå, trenger ikke involvering av ekspertkunnskap. En lege kan gjennom kjenne igjen en symptomer på en sykdom, og kanskje behandle på stedet.
- *Kompliserte risikoer* - Behovet for involvering av ekspertkunnskap øker, dersom legen ikke klarer å kjenne igjen symptomer eller behandle pasienten, må han kanskje sendes videre til en spesialist på det gjeldende feltet.
- *Usikre risikoer* - Behovet for ekspertkunnskap øker nok en gang, og det blir behov for tverrfaglig kompetanse med ulike bakgrunner for å se ulike sider av risikoene. Her må ofte interessenter inkluderes, for å eventuelt oppdage interessekonflikter eller konflikter knyttet til kunnskapssyn.
- *Tvetydige risikoer* - Her er all informasjon nødvendig, og det blir behov for å involvere alle deler av samfunnet; både eksperter, lekfolk, interessenter og innbyggerne. Det legges ofte opp til offentlige diskurser som stortingshøringer

og fokus i media, slik at lekfolk også har mulighet til å være med på å påvirke beslutningen og håndteringen av risikoen.

Graden av kompleksitet, usikkerhet og tvetydighet vil påvirke hvor mye informasjon vi føler behov for, og hvor mange eksperter, interessenter og stakeholders vi føler er nødvendige for å vurdere og tolke risikoen riktig. Dersom vi feiltolker risikoen, f.eks. ved at vi unnlater å involvere ekspertkunnskap knyttet til en kompleks risiko, når vi burde det for å skape en bredere og riktigere forståelse, vil vurderingene vi gjør videre i prosessen bli gjort og vurdert på et feil grunnlag. Det kan også føre til at beslutningsalternativene og håndteringstrategiene blir totalt feil, og at det kan oppstå katastrofale hendelser. Stakeholder involvement er dermed en veldig viktig og avgjørende del av prosessen, og har stor betydning for resultatet av risikostyringsprosessen. Fordelen med stakeholder involvement er at de kan inkluderes gjennom alle trinnene av risikostyringsprosessen dersom man ser behovet for det.

Kontinuerlig prosess

Risk governance er en kontinuerlig prosess som vi hele tiden må jobbe med kontinuerlig ettersom vi lever i et så dynamisk og komplekst samfunn. Så snart det oppstår hendelser, trusler, risikoer og usikkerheter må arbeidet med risikostyring, håndtering og beslutninger starte om igjen. Dersom risikoene endrer karakter (går fra kompleks til usikker, eller usikker til tvetydig), må risikoanalysen og risikovurderingene gjøres om igjen.

Vi kan ikke gjøre en risikovurdering og si oss fornøyde med resultatet, for så iverksette tiltak og styringsprosesser som vi aldri endrer eller gjør noe med igjen. Disse styringsmetodene og tiltakene vil bli utdaterte ettersom nye risikoer oppstår, og må kontinuerlig erstattes ettersom globaliseringen og kunnskap knyttet til risiko utvikler seg. Vi lever i et dynamisk samfunn hvor tilgjengelig informasjon knyttet til risiko og usikkerhet hele tiden oppdateres, og det er en

viktig del av risikostyringen og en viktig del av å opprettholde og skape et robust samfunn å følge med på denne utfordringen. Dersom vi ikke klarer det, vil vi heller ikke klare å beskytte oss mot de nye risikoene etter hvert som de utvikles.

Ord: 1617

Seksjon B

Oppgavesettet består av to seksjoner, seksjon A og B. Kandidaten skal velge en av seksjonene, og besvare begge oppgaver i valgt seksjon.

3 Risk,safety og security

Vis hvordan ulike perspektiver på risiko og safety og security kan integreres i en og samme modell og hvordan dette kan komme til uttrykk i praktisk politikk. Illustrer med eksempler.

Skriv ditt svar her

Ord: 0

4 Organizational accidents and Risk Governance

Drøft hvilken av de to organisatoriske risikoteoriene («Normal Accident»- teorien og «High Reliability Organizations» - teorien) som ligger nærmest Risk Governance modellen. Begrunn svaret!

Skriv ditt svar her

Ord: 0