Risk Manager (RM)
Dette dokumentet gjengir krav til kandidatens kompetanse i Normativt dokument for sertifisering av Risk Manager med utdypninger. Disse kravene vil danne grunnlag for utarbeidelse av eksamensoppgaver og bedømming av eksamensbesvarelser. I listen under benyttes følgende koder for krav til kunnskap:

A = Kjennskap til, oversikt.
B = Forstå
C = Kunne anvende
D = Analysere resultater og evaluere dem

Svart tekst er det opprinnelige Normative Dokumentet, blå tekst er tillegg i denne pensumlisten.

Oppgave beskrivelse for Risk Manager	Relatert kunnskap og ferdighet	Lære taksonomi (nivå)
A	**Risikostyring, generelt**	
Anvende ledelsesmodeller, anvendelse av alle aspekter av ISO 31000. Grunn-leggende statistikk i risikostyring	**Grunnleggende risikostyringsbegreper** • Risk Manager ansvar og myndighet, posisjon i organisasjonen • Bruk av risikostyring i organisasjonens beslutningsprosesser • Reaktiv og proaktiv risikostyring • Holdning til risiko: Risikoappetitt og risikoaversjon • Kost / nytte analyse i risikoevaluering. Vurdering av kost/nytte ved tiltak, prioritering mot andre tiltak. • Begrepet «Risikoeier» og tilhørende ansvar • Risiko-policy, policy-elementer: Hvem skal utarbeide politikken. Eksempler på politikk. • Etablering av risikokriterier, typer av risikokriterier. Eksempler på kriterier for akseptabel risiko/ ikke akseptabel • Positiv risiko og negativ risiko, muligheter og trusler. SWOT analyser. Negativ og positive elementer knyttet til samme risiko. • Risikostyringsdokumentasjon, risikoregister. Eksempel på innhold i risikoregister. Ansvar for vedlikehold. Annen dokumentasjon knyttet til risikostyring. • Integrering av risikostyring i det eksisterende systemet for ledelse • Juridiske aspekter av risiko, overenstemmelse med juridiske krav. Produktansvar, formuesansvar, garantiansvar. • Individets oppfattelse av risiko	**C**
	Risikostyringsstandarder og lovverk • NS-ISO 31000 “Risikostyring – Prinsipper og retningslinjer”. Detaljert kunnskap om denne standarden. • NS-5814 ”Krav til risikoevaluering”. Hva standarden dekker. • Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften). Kunnskap om hvem forskriften gjelder for, hjemmel, og spesielt § 5 om risiko.	**D** **A** **B**

	Risikostyringsprosessen (NS-ISO 31000) • Den iterative modellen for risikostyring, syklisk prosess for risikoendring. Hvem er ansvarlig for iterasjonene. Hvor ofte skal prosessen gjentas? • Bestemmelse av konteksten: Identifikasjon av eksterne og interne risikotakere og deres risiko, negative og positive. Identifikasjon av risikotakere med spesielt risikopotensiale, negativt og positivt. Identifikasjon av tilstander som påvirker risiko. Dette favner vidt, kartlegging av alle parter og forhold som påvirker risikoen. • Kommunikasjon og konsultasjon: Hensikt og planlegging. Kontakt med risikoeiere, skaffe til veie ekspertise innen risikoanalyse, kommunikasjon med ulike berørte parter om spesifikk risiko. Fastsettelse av en kommunikasjonsplan, ansvar for at en slik plan blir laget og innfridd. • Risikoidentifikasjon: Analyse av potensiell risiko relater til utvalgte risikotakere. Verktøy for risikoidentifikasjon: "Brain storming", årsak / virkning diagram, Affinitetsdiagram. Risikoregister. Identifiserte risikoer føres opp i risikoregisteret med ID nr., risiko eier, etc. Eksempler. • Risikoanalyse: Valg av egnet analysemetode for ulike typer risiko. Metoder er gjennomgått i ISO 31010, men de mest aktuelle er nevnt i del B i dette dokumentet. Utredninger er også en metode. Presentasjon av resultater grafisk i matriser, e.l. • Risikoevaluering: Velge risiko for videre behandling. Vurdering av hvor det er mulig å oppnå positive resultater, foreløpig kost / nytte vurdering. • Risikohåndtering: Negativ risiko: Redusere sannsynlighet og/eller redusere konsekvens. Positiv risiko (mulighet): Øke sannsynlighet og/eller øke konsekvens. Kobling av positive og negative sider ved samme risiko. • Overvåking og gjennomgåelse: Hensikt og planlegging. Gjennomgåelse av prosesser, dokumentasjon av analyser og aktiviteter, verifisere resultater. • Oppdatere risikoregisteret. Ansvarsfordeling av oppdateringen, risikoeier / Risk manager	**D**
	Ledelsessystemer • Ledelsessystemer som plattform for å etablere risikostyring. Krav til grunnleggende ledelsessystemer for å kunne implementere risikostyring. • NS-EN ISO 9001:2015 "Ledelsessystem for kvalitet – Krav" og NS-EN ISO 14001:2015 "Ledelsessystem for miljø – Spesifikasjon med veiledning". Kjennskap til sentrale funksjoner.	**A**
	Grunnleggende statistikk og sannsynlighetsteori • Statistikk: Sentraltendens: Aritmetisk middel (middelverdi), mode. Enheter for spredning: Varians, standardavvik, range. Histogrammer og fordelinger, Normalfordelingen. «De store talls lov». Binominalfordelingen. S-kurver. Egenskaper ved fordelingene, akkumulert fordeling/histogram til S-kurve. • Sannsynlighet, sannsynlighetsklasser i risikomatriser • Konsekvens, konsekvensklasser i risikomatriser.	**B**

B	Risiko analyse	
Være i stand til å analysere risiko med hensyn på størrelse, trusler og muligheter. Være i stand til å velge passende analysemetoder.	**Grunnleggende risikoanalyse** • Risiko som et produkt av sannsynlighet og konsekvens • Tilfeller av ikke-linearitet hvor produktet av sannsynlighet og konsekvens ikke kan benyttes som uttrykk for risiko. • Spesiell behandling av tilfeller hvor sannsynlighet er svært liten men konsekvensen er ekstrem.	**D**
	Generelle risikoanalyse metoder • **Risikomatriser**: Fremstilling av analyseresultater i ulike risikomatriser. Avhengigheter mellom positiv og negativ risiko. Presentasjonsformer i matriser. Eksempler. • **ROS-metoden**: Risiko og sårbarhetsforskning, Norges forskningsråd. Egen publikasjon fra forskningsrådet. • **NSO-metoden**: Risikoanalyse, Næringslivets Sikkerhetsorganisasjon. Gjelder industrivern. Egen publikasjon fra NSO. • **Grovanalyse**: (Preliminary hazard analysis): Anvendelsesområder. Systematikk, skjema og presentasjon. Styrker og svakheter. Eksempel. • **FMEA / FMECA**: Feilmodi- og feileffektanalyse (Failure Modes and Effects Analysis) og Feilmodi-, kritikalitet- og feileffektanalyse (Failure Modes, Effects and Criticality Analysis). Forskjell mellom FMEA og FMECA. Anvendelsesområder og begrensninger. Systematikk og skjemaer. Styrker og svakheter. Eksempel. • **Feiltreanalyse** (Fault tree analysis): "Og" og "Eller" porter. Trestruktur. Hensikt med analysen og bruksområder. Dataprogram støtte og beregning av sannsynligheter. Styrker og svakheter. Eksempler. • **Hendelsestreanalyse**: (Event tree analysis). Bruksområde, hensikt med analysen. Forplantning av hendelser, generasjonsstruktur. Beregning av sannsynlighet for ulike slutthendelser. Grafisk fremstilling og dokumentasjon av resultater. Styrker og svakheter. Eksempler. • **Strukturert hva-hvis** (Structured what-if, SWIF): Bruksområder og hensikt. Etablering av struktur og parametre. Metodebeskrivelse. Styrker og svakheter. • **Sikker jobbanalyse:** (Safe job analysis): Skjemaer, dokumentasjon og myndighet til å starte arbeid. • **Stokastisk simulering**: Monte Carlo simulering. Forskjellen på deterministisk og stokastiske systemer og simulering. Tilfeldige tall. Generatorer for tilfeldige tall. Dataprogrammer for simulering. Hensikt og bruksområde for Monte Carlo simulering. Eksempel. Forstå prinsippet bak simuleringen: Å kunne regne med fordelinger. Bruksområder. Prinsippet bak en tallgenerator som lager tilfeldige tall, tilpasning av tallgeneratoren til en gitt fordeling/histogram.	**C**
	Andre risikoanalysemetoder • **NS-ISO/IEC 31010** "Risikostyring – Metoder for risikovurdering". Oversikt over metodene. • **HAZOP-analyse** (Hazard and operability analysis): Bruksområde og hensikt med analysen. Ledeord og og parametre. HAZOP leders oppgaver. Dokumentasjon av	**B**

	resultater. Styrker og svakheter. Eksempel. • **HAZID**: Fareidentifikasjon (Hazard Identification): Bruk av sjekklister i operasjoner. Dokumentasjon av resultater. Styrker og svakheter. • **HACCP-analyse** (Hazard Analysis Critical Control Point): Identifikasjon av kritiske kontrollpunkter. Bruksområder. Bruk av metoden i prosesstyring. Styrker og svakheter.	
C	**Psykologiske sider av risiko**	
Anvende metoder for å redusere den menneskelige faktor. Menneskelig feilrate. Begrepet omdømme, Hindre tap av omdømme.	**Menneskelig faktor** • Menneskelige faktorers rolle i ulykker. Hva en menneskelig faktor er og ikke er. • Opplæring for å minimalisere den menneskelige faktoren. Opplæring for utsatte stillingskategorier. • Håndtering av kriser og kaos, overbelastning av informasjon, unngåelse av panikk. Metoder for trening i situasjoner som kan lede til panikk. • "Menneske/maskin"-samspill. Intuitive grensesnitt.	**C**
	Risiko for tap av omdømme • Omdømmets betydning for organisasjonen, negativ omtale i media. • Faktorer som kan føre til tap av omdømme: Korrupsjon, lovbrudd, uetisk adferd, mangel på samfunnsansvar. Metoder for å forebygge slike faktorer, avdekke slike faktorer på et tidlig stadium. • Beskytte organisasjonens omdømme: Beredskap mot anklager, tilgjengelighet av korrekt informasjon, håndtering av media, medietrening.	**D**
D	**Prosjektrisiko**	
Anvendelse av beredskapsplaner i prosjekter og estimering av kostnad ved hjelp av Monte Carlo-simulering.	• Bruk av Strukturert hva-hvis-metoden i prosjekter. Hva er strukturen? Hvilke parametere benyttes? • Kompleks kostnadsestimering, bruk av Monte Carlo simulering. Estimering av prosjekter, metode for å finne frem til prosjektets usikkerhet.	**C**
E	**Sikkerhet for mennesker**	
Forstå faktorer som skaper sikkerhet for mennesker.	• Skape en sikkerhetskultur. Informasjonsmøter. H-verdi. Tema for informasjonsmøter, hyppighet, deltakere. Registrering av hendelser, dokumentasjon og oppfølging av hendelser. Styrke og svakhet ved H-verdi for registering av hyppighet av hendelser. • SN-BS OHSAS 18001 "Styringssystemer for arbeidsmiljø - Krav". Oversikt.	**C** **A**
F	**Objektsikkerhet**	
Anvende metoder for å avdekke mulige trusler og beskyttelse mot forsettlig skade.	• Forsettlig skadeverk: Innbrudd, tyveri, sabotasje, spionasje. Hvem ar aktørene og hva er motivasjonen. • Beskyttelse mot forsettlig skadeverk: Adgangskontroll, tidsforsinkende utstyr (låssystemer) identifikasjonsmetoder, biometriske identifikasjoner, intern televisjon, utstyr for deteksjon av inntrengere og alarmer, brannbeskyttelse og alarmer. Personvern. Personvern er sentralt, når kan man bruke ulike metoder og til hva. Låssystemer er bare tidsforsinkende, alle låser kan forseres. Lovligheten av å	**C**

	benytte biometriske metoder til identifikasjon. Lovlighet ved å benytte intern televisjon • Metoder for å kartlegge sårbarhet mot trusler, trusselbildet, vurdering av trusselpotensiale. En metode er vist til i neste punkt. • Objekt- og informasjonssikkerhet: Metode for risiko- og sårbarhetsanalyse, NTNU. Egen publikasjon fra NTNU.	
	Lov om forebyggende sikkerhetstjeneste. Hvem loven gjelder for, hovedpunkter. • Personopplysningsloven med forskrift. Hvem loven gjelder for, hovedpunkter. • NS 5831:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring • NS 5832:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktende uønskede handlinger – sikringsrisikoanalyse	**A**
G	**Informasjonssikkerhet**	
Anvende metoder for identifikasjon av trusler, beskyttelse mot trusler, systemutforming.	**Trusler for informasjonssystemer** • Virus: Trojanere, ormer, RAT (remote access Trojans), Styring av PC-grupper, virusspredning, "logiske bomber" (tidsstyrt virus). Hovedtrekk ved de ulike gruppene, hvem er aktørene, hva er motivasjonen. • Spionasje: Spyware, ransomware. «Løsepengevare» for å åpne passordbelagte filer. • "Phishing". Lure forbrukere. DOS-angrep (denial of service). Løsepenger for å slutte DOS angrep	**B**
	Beskyttelse av informasjonssystemer • Administrative hjelpemidler: Systemarkitektur (design av intranet, extranet, porter), back-up systemer, adgangskontroll (passord), autorisert adgang til filer, kryptering av data, testing av sikkerheten. Software-verktøy: Antivirusprogrammer, anti-adware og anti-spyware programmer, "Honey pots" (hacker feller). • Hardware-verktøy: Brannmur, inntrengningsdetektorer, uavbrutt kraftforsyning.	**B**
	Standarder / forskrifter om systemer for informasjons-sikkerhet • NS-ISO/IEC 27001 "Informasjonsteknologi – Sikkerhetsteknikk - Krav" • NS-ISO/IEC 27002 "Informasjonsteknologi – Sikkerhetsteknikk – Administrasjon av informasjonssikkerhet" • NS-ISO/IEC 27005 "Informasjonsteknologi – Sikringsteknikker – Risikostyring av informasjonssikkerhet" • Forskrift om bruk av informasjons- og kommunikasjonsteknologi. Med relasjon til risiko. • COBIT: Control Objectives for Information and related Technology. Hensikt med denne amerikanske loven, hvem den gjelder for.	**A**
	Kriminelle handlinger relatert til IT sikkerhet • Deteksjonssystemer, transaksjonslogger. • Fastlagt rapporteringskanal, instruksjoner for å sikre bevis. En utpekt og spesielt trenet person som skal kontaktes ved sikkerhetsbrudd. • Undersøkelse og beslutning om straffeforfølgning. Frysing	**A**

	av bevis, sørge for at bevis er pålitelig i en straffeprosess.	
H	**Finansiell risiko**	
Anvende mekanismene om vinning og tap, typer av finansiell risiko, pålitelig regnskaps-rapportering	**Finansiell risiko og risikokapital** Hvordan man kan beskytte seg mot de ulike typer finansiell risiko: • Kredittrisiko: Manglende betaling • Portfoliorisiko: Samling av ulike finansielle instrumenter. • Forandring i valutakurser • Forandring i rentenivå • Likviditetsrisiko: Tilgjengelighet av kontanter • Ansvarsrisiko • Risikokompensasjon ved forsikring • Investeringsrisiko	**B**
	Regnskap • Pålitelig regnskapsrapportering • Svik. Hva fører til svik i en organisasjon. Hvordan kan det utføres. • COSO-rapporten. Internkontroll med fokus på økonomi. Hovedtrekk. • Sarbanes Oxley Act. USA-lov om pålitelig regnskaps-rapportering. Hvem den gjelder for.	**B**
I	**Beredskap - evne til å fortsette driften**	
Anvende system for beredskap, forstå begrepet "business continuity", evne til fortsatt drift.	**Beredskap** • Beredskapsplanlegging, øvelser i å håndtere nødsituasjoner. Planlegging av øvelser, rapportering av resultater. • Back-up løsninger, testing av løsninger • Kriterier for å iverksette back-up løsninger. Akseptert tap før back-up løsninger aktiveres.	**C**
	Evne til fortsatt drift • Umiddelbar handling • Midlertidig drift • Normaliseringsfasen	**B**