Co-funded by the Erasmus+ Programme of the European Union

InCyT træningsmodul

Informationssikkerhed for ledere **Enhed (modul) 4, uge 7 og 8** **Enhedens (modul) navn: Cyberrisiko og modstandsdygtighed**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑**Andet**
Læringsansvarlig	• Simon Tjoa • Peter Kieseberg
Læringsaktivitetsmål	1. Deltagerne kender grundlaget for risiko- og resiliensstyring 2. Deltagerne er i stand til at udføre forretningskonsekvensanalyse og risikoanalyse 3. Deltagerne kan udlede modforanstaltninger og sikkerhedsbeslutninger ud fra resultaterne af analyser
Færdigheder, der skal opnås	• IS 1, IS 3 • MS 1
Varighed af læringsaktivitet	2 uger • Uge 7 (2 timer) • Uge 8 (2 timer)
Læring krav	***Hvad skal der til?*** • Grundlæggende ledelsesevner • Grundlæggende IT-færdigheder • Grundlæggende sikkerhedsfærdigheder

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Kort information om modulet

Beskrivelse
Perfekt sikkerhed er ikke mulig. Når man ved dette, er det vigtigt at træffe informerede beslutninger om, hvordan man bruger penge til de rigtige sikkerhedsforanstaltninger. Cyberrisiko- og resiliensstyring giver et vigtigt sæt værktøjer og teknikker til at vurdere den aktuelle sikkerhedstilstand i en organisation og til at planlægge kontroller for at holde informationssikkerhedsrisikoen på et acceptabelt niveau.

Lærematerialets indhold

Uden at tage risici er det umuligt at lave forretning. Derfor giver risikostyring og de tilsvarende værktøjer og teknikker en systematisk måde at håndtere risiko på. Spørgsmål som hvor meget sikkerhed er nok, eller hvilken modforanstaltning der skal implementeres først, besvares af risikostyring. Risikostyring er således en vigtig aktivitet for at muliggøre informerede beslutninger. Vigtige standarder og bedste praksis, der behandler dette vigtige emne, omfatter ISO 27005, ISO 31000 eller BSI 200-3.

Før du ser nærmere på risikostyringsprocessen, er det vigtigt at definere væsentlige termer:

- **Sårbarhed:** "Svaghed i et informationssystem, systemsikkerhedsprocedurer, interne kontroller eller implementering, der kunne udnyttes eller udløses af en trusselkilde."[1]
- **Kontrol:** "En beskyttelses- eller modforanstaltning foreskrevet for et informationssystem eller en organisation designet til at beskytte fortroligheden, integriteten og tilgængeligheden af dets oplysninger og til at opfylde et sæt definerede sikkerhedskrav."[2]
- **Trussel:** "Enhver omstændighed eller begivenhed med potentiale til at have en negativ indvirkning på organisatoriske operationer (herunder mission, funktioner, image eller omdømme), organisatoriske aktiver, enkeltpersoner, andre organisationer eller nationen gennem et informationssystem via uautoriseret adgang, ødelæggelse, offentliggørelse, ændring af information og/eller lammelsesangreb."[3]
- Risiko: "Et mål for, i hvilket omfang en virksomhed er truet af en potentiel omstændighed eller begivenhed, og er typisk en funktion af: (i) den negative påvirkning eller omfanget af skade, der ville opstå, hvis omstændigheden eller begivenheden indtræffer; og (ii)

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control
[3] https://csrc.nist.gov/glossary/term/threat

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

sandsynligheden for forekomst."[4]
"effekt af usikkerhed på mål"[5]

Ud fra definitionen af ISO 31000 ("effekt af usikkerhed") kan vi udlede, at risici kan have positive og negative virkninger. Ofte, hvis risici har positive virkninger, omtales de som muligheder.

Den generelle risikostyringsproces starter med omfanget, konteksten og kriterierne. Da ikke alle risici for alle aktiviteter kan analyseres, er det vigtigt at prioritere og beslutte, hvilke services, processer og organisatoriske enheder der skal indgå i vurderingen. At have et tilstrækkeligt omfang er afgørende for at sikre valide resultater på den ene side og en rimelig indsats på den anden side. Konteksten er det indre og ydre miljø. Fastlæggelsen af risikokriterier er vigtig for at sikre en og gentagelig proces, som fører til sammenlignelige resultater. Kriterierne bør defineres på en måde, så forskellige personer er i stand til at vurdere risici på en fælles måde.

Eksempler på kriterier omfatter indvirkningskriterier (f.eks. lav, middel, høj) for forskellige dimensioner, såsom økonomi, omdømme eller sundhed.

I det følgende præsenteres et eksempel på OCTAVE Allegro vedrørende omdømme og kundepåvirkninger:

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Figur 1: Målekriterier for omdømme[6]

Efter definitionen af risikokriterier og omfanget er det første skridt at identificere risici. Risikoidentifikation er afgørende, da kun de risici, som identificeres, kan vurderes. Det giver derfor mening at sammenligne identificerede trusler med trusselslister over ISO 27005, MEHARI eller andre bedste praksisser eller standarder.

Der findes forskellige teknikker [7]til at identificere risici, såsom brainstorming, Delphi-teknik,

[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Failure Mode and Effects Analysis (FMEA) eller Hazard and Operaability studies (HAZOP).

I næste trin risikoanalyse opnås en bedre forståelse af de identificerede risici. Derfor bestemmes forekomstsandsynlighed/-hyppighed og påvirkning/konsekvenser. For at fastlægge konsekvenser er det vigtigt at definere en systematisk måde, hvordan påvirkninger vurderes. Ofte er et kvalitativt mål (f.eks. lav, medium, høj) lettere at bruge end kvantitative mål.

Risici visualiseres ofte i en såkaldt risikomatrix, som fremhæver risikoen ved at bruge sandsynlighed og påvirkning som akser.

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Figur 2: Risikomatrix [Kilde Wikipedia][8]

I næste trin vurderes risiciene. Det betyder, at resultaterne af det foregående trin vurderes til at afgøre, om der skal træffes foranstaltninger. Endvidere sker en prioritering af risici.

Dernæst fastlægges en af de fire hovedstrategier til at håndtere risici:

- Risikoaccept: Dokumenter og overvåg risiko, hvis risikoen ligger inden for organisationens risikovillighed
- Risikooverførsel: aktierisici (f.eks. forsikring, joint venture)
- Risikoundgåelse: fjern risikokilden (f.eks. luftspalte)
- Risikobegrænsning: reducer sandsynligheden for påvirkning eller hændelse (f.eks. adgangskontrol)

Efter fastlæggelse af foranstaltninger vurderes det, om den resterende risiko er acceptabel, eller der skal træffes yderligere foranstaltninger.

Som understøttende aktiviteter ved siden af den primære risikovurderingsproces finder risikokommunikation (dvs. kommunikation med relevante interessenter), risikoovervågning og

[7]Cmp. https://www.iso.org/standard/72140.html
[8] https://en.wikipedia.org/wiki/Risk_matrix

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

risikorapportering sted.

Da ikke alle risici kan tages i betragtning, fokuserer forretningskontinuitet og robusthed i modsætning til risikostyring på kritiske aktiviteter i stedet for individuelle risici. På denne måde er det muligt at forberede sig på ukendte risici med lav sandsynlighed/høj indvirkning.

For at sikre et effektivt forretningskontinuitetsprogram er støtte fra topledelsen afgørende. En vigtig artefakt, der fremhæver vigtigheden af forretningskontinuitetsstyring, er forretningskontinuitetspolitikken. I dette dokument er ledelsens buy-in formelt udtrykt. Yderligere fremhæver dokumentet omfanget og målene for forretningskontinuitetsaktiviteterne, vigtige roller og ansvarsområder (f.eks. business continuity manager) samt den operationelle ramme, der bruges til at udføre programmet. Det skal understreges, at omfanget ikke bør være for bredt for at sikre, at både analysens kompleksitet og indsatsen ikke bliver for høj.

For at forstå effekterne af serviceforstyrrelser på forretningen og have et godt grundlag for planlægning af genopretningstiltag, gennemføres forretningskonsekvensanalyser. Det er det centrale værktøj i forretningskontinuitetsprocessen og fanger relevansen/betydningen af produkter/ydelser. Ud over kritikaliteten af produkter/tjenester bestemmes og vurderes deres afhængigheder.

Vigtige nøgletal, som bruges ved udførelse af en forretningskonsekvensanalyse omfatter:

- **MAO (maksimalt acceptabelt udfald):** "tid det ville tage for negative påvirkninger [...], som kan opstå som følge af ikke at levere et produkt/tjeneste eller udføre en aktivitet [...], bliver uacceptable"[9]
- **RTO (recovery time goal):** "periode efter en hændelse […] inden for hvilken et produkt og en service […] eller en aktivitet […] genoptages, eller ressourcer […] er gendannet"[10]
- **RPO (recovery point goal):** "punkt, hvortil information […] brugt af en aktivitet […] gendannes for at gøre det muligt for aktiviteten at fungere ved genoptagelse"[11]

I det første trin identificeres de mest kritiske eller væsentlige produkter og tjenester. Efter identifikationen vurderes det, hvilke skader der vil opstå over tid, hvis et bestemt produkt eller en bestemt ydelse bliver forstyrret eller afbrudt.

Den efterfølgende figur viser, hvordan virkningen over tid kunne fanges i et regneark.

[9]MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10]RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[11]RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Endvidere foretager de forretningsmæssige konsekvensanalyseundersøgelser, hvorfra processer, aktiviteter og ressourcer relevante tjenester er afhængige. På denne måde kan vigtige nøgletal, såsom restitutionstidsmålsætningen, restitutionspunktmålsætningen og det maksimalt acceptable udfald, bestemmes.

Efter at have kendskab til kritikaliteten af processer, tjenester og ressourcer, udarbejdes forretningskontinuitetsstrategier. Strategier omfatter blandt andet diversificering (f.eks. aktiviteter på geografisk adskilte steder), replikering (f.eks. kopiering af data for at gendanne andre steder) eller underleverandører (f.eks. brug af tredjepartstjenester).

Baseret på strategierne bliver der skrevet forretningskontinuitetsplaner, som understøtter organisationer i at reagere på en effektiv måde efter en hændelse. For at kunne bruges i pressede situationer er det afgørende, at planerne er skrevet i overensstemmelse hermed. Det betyder, at planer kun skal indeholde den information, der er relevant under håndtering af en hændelse. Desuden skal informationen være hurtig at forstå. Der bør derfor anvendes klare og handlingsorienterede tjeklister.

Typiske forretningskontinuitetsplaner indeholder oplysninger om formål, omfang, hændelsesstyringsstruktur, roller og ansvar, planaktivering, genopretningsordninger og kontaktoplysninger.

For at øve og kontrollere planernes tilstrækkelighed anvendes forskellige typer øvelser. Dette kan enten være diskussionsbaserede øvelser, såsom skrivebordstjek eller bordøvelser eller tekniske øvelser, såsom test af gendannelse af bestemte systemer.

Spørgsmål :

Se Word-dokumenter

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Vedhæftede filer:

Se Powerpoint- og videofiler

Referencer:

- ISO 22301:2019, Sikkerhed og robusthed — Forretningskontinuitetsstyringssystemer — Krav
- ISO 22313:2020, Sikkerhed og robusthed — Forretningskontinuitetsstyringssystemer — Vejledning i brugen af ISO 22301
- ISO/TS 22317:2021, Sikkerhed og robusthed — Forretningskontinuitetsstyringssystemer — Retningslinjer for forretningskonsekvensanalyse
- ISO/TS 22331:2018, Sikkerhed og robusthed — Forretningskontinuitetsstyringssystemer — Retningslinjer for forretningskontinuitetsstrategi
- ISO/TS 22332:2021, Sikkerhed og robusthed — Forretningskontinuitetsstyringssystemer — Retningslinjer for udvikling af forretningskontinuitetsplaner og -procedurer
- ISO 31000:2018, Risikostyring — Retningslinjer, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risikostyring — Risikovurderingsteknikker

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.