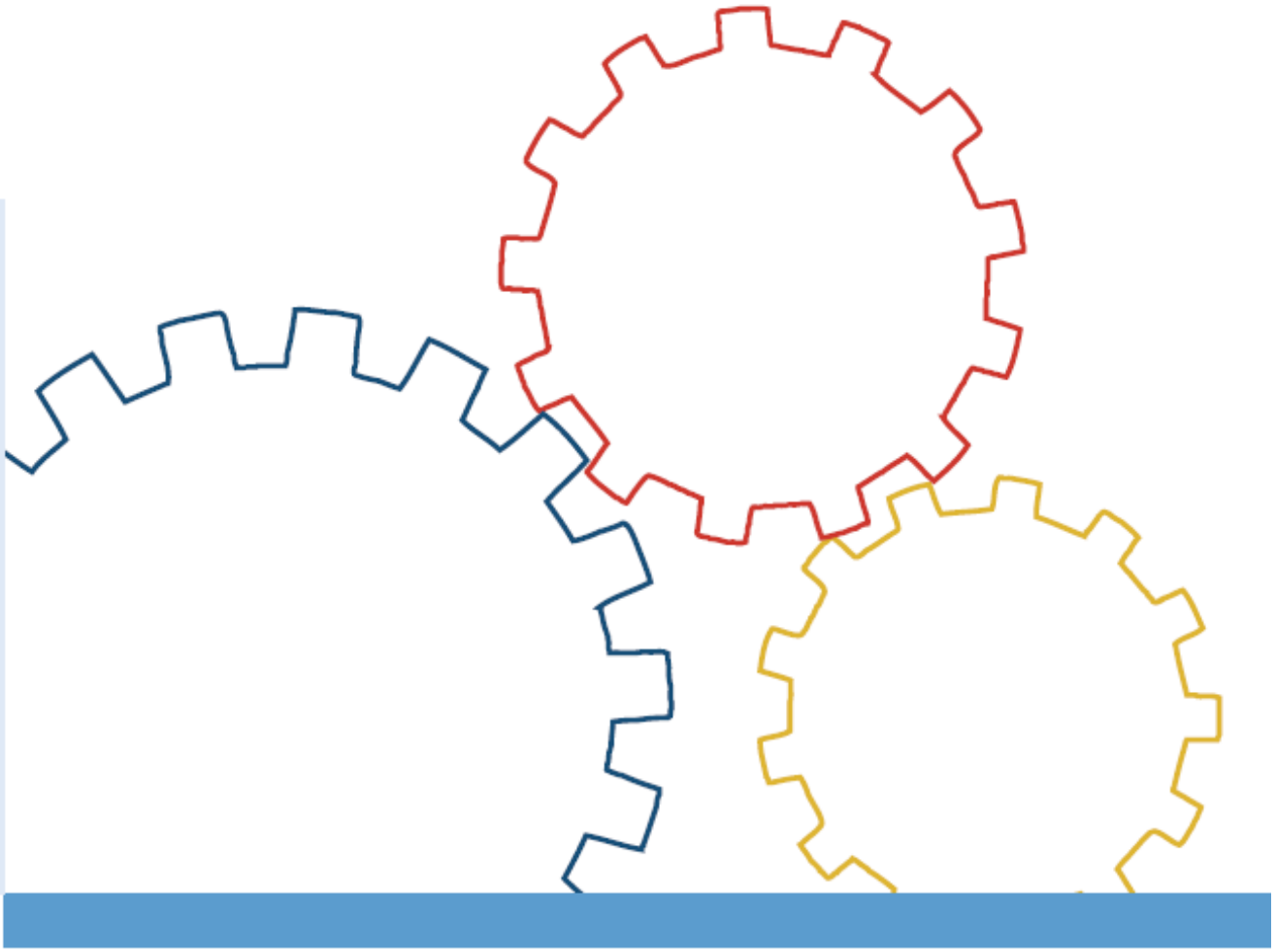
Bundesamt
für Sicherheit in der
Informationstechnik

BSI standard 100-4
Hädaolukordade haldus



www.bsi.bund.de/gshb

Versioon 1.0

1 Sissejuhatus

1.1 Versiooni number

Seis	Versioon	Koostaja
November 2008	1.0	BSI

1.2 Eesmärk

Ametiasutustel ja ettevõtetel tuleb silmitsi seista üha uute riskidega, mis võivad pärssida kas tootmist või klientidele suunatud teenuse võimalikult kiiret osutamist. Olukorra kasvavale keerukusele aitavad kaasa ühiskondlikud ja majanduslikud arengud nagu üleilmastumine, laienevad võrgusüsteemid, tsentraliseerimine, automatiseerimine väljast tellimine ja osakondade välismaale kolimine. Kuna äriprotsessid muutuvad aina keerukamaks ning nende sõltuvus nii infotehnoloogiast kui ka välistest teenusepakkujatest kasvab pidevalt, võivad sellised sündmused nagu tulekahju, üleujutus või infotehnoloogia hädaolukord, teenusepakkuja, tarnijate või personali väljalangemine jms viia tõsiste tagajärgedeni. Lisaks muule kasvab pidevalt ka pandeemiate, halbade ilmastikuolude ja terrorismi oht.

Hädaolukordade haldus on haldusalane protsess, mille eesmärgiks on organisatsiooni toimimist ohustavate tegurite võimalikult varajane tuvastamine ja vastumeetmete rakendamine. Ettevõtte ja ametiasutuse funktsioonide säilimiseks ja nende toimimise tagamiseks tuleb kasutusele võtta sobivad ennetavad meetmed, mis peaksid ühelt poolt tõstma tööprotsesside robustsust ja hädaolukorrakindlust ning teistelt poolt tagama võimalikus hädaolukorra- või kriisiolukorras kiire ja sihipärase reageerimise. Hädaolukordade halduse kontseptsioon hõlmab planeeritud ja organiseeritud lähenemist, mis peaks tagama institutsiooni (ajalis-)kriitiliste tööprotsesside vastupanuvõime jätkusuutliku kasvu, adekvaatse reageerimise ohtudele ja võimaluse taas tööprotsessidega võimalikult kiiresti jätkata. Hädaolukordade haldus kannab muuhulgas ka veel nimetust Business Continuity Management (BCM) ehk tegevuse järjepidevuse haldus.

Hädaolukordade halduse eesmärk on kindlustada, et olulised tööprotsessid ei katkeks ka kriitilistes situatsioonides või katkeksid ainult lühikeseks ajaks ning tagada, et isegi suuri kahjusid kaasa toovad olukorrad ei seaks kahtluse alla institutsiooni majanduslikku edasikestmist. Seetõttu on siinkohal määravaks terviklik lähenemine. Vaadelda ei tule ainult infotehnoloogia ressursse, vaid kõiki aspekte, mis on olulised kriitilise tähtsusega tööprotsesside jätkamiseks olukorras, kus tekib mingi kahju. IT-hädaolukordade haldus on hädaolukordade halduse üks osa.

Käesolevas BSI standardis 100-4 esitleme teile metoodikat, mille abil on võimalik juurutada ja käigus hoida institutsioonisisest hädaolukordade haldust. Dokumendis kirjeldatava metoodika aluseks on BSI standard 100-2 [BSI2] ja selles kirjeldatud IT-etalonturve. Käesoleva standardi juurutamisega täies mahus ja sellega kokkukäivate asjakohaste IT-etalonturbe moodulite ellurakendamine loob hädaolukordade halduse, mis täidab ka madalama tehnilise suunitlusega standardeid nagu British Standard BS 25999 Part 1 ja 2 täiel määral.

Riigiasutusi ja -ettevõtteid hõlmava hädaolukorra- ja kriisihalduse väljatöötamise vajadust käsitleb projekt nimega Schutz Kritischer Infrastrukturen in Deutschland [KRI] (Saksamaa kriitilise tähtsusega infrastruktuuride kaitse) ning selle detailsem käsitlus on kirjas kavades Umsetzungsplan KRITIS (KRITISe rakenduskava) ja Umsetzungsplan Bund (Riiklik rakenduskava). Katastroofide vastast kaitset puudutav väline hädaolukorra- ja kriisihaldus kuulub eranditult Saksa elanikkonna kaitse ja katastroofiabi riikliku ameti (Bundesamt für

Bevölkerungsschutz und Katastrophenhilfe, BBK) kompetentsi. Ameti eesmärgiks on tagada rahvastikukaitse ja tsiviilkaitse. Kumbki nimetatud valdkondadest ei kuulu BSI standardis vaadeldavate teemade hulka, vaid on täiendavad valdkonnad.

1.3 Sihtgrupid

Käesolev dokument on suunatud hädaolukorraametnikele ja tegevuse järjepidevuse tagamise halduritele (Business Continuity Manager), kriisistaabi liikmetele, turvaspetsialistidele, turvavolinikele, turvaekspertidele ja turvanõustajatele, kes on kursis hädaolukordade ja kriiside halduse tehnilise ja mittetehnilise poolega. Selles dokumendis kirjeldatud metoodika rakendajad peaksid tundma IT-etalonturbe meetodit, mida kirjeldatakse BSI standardis 100-2. Sobiv hädaolukordade haldus on vajalik nii suurtele kui ka väikestele institutsioonidele. Efektiivne ja otstarbekas hädaolukordade haldus ei pea olema ilmtingimata kallis. Kuna väiksed ja keskmise suurusega asutused on reeglina ka madalama keerukusastmega ja neil ei ole üleliia palju erinevaid asukohti, tööprotsesse ega sõltuvussuhteid, on ka vastavate asutuste hädaolukordade halduse kulud tunduvalt väiksemad. Kuid sellele vaatamata võib just niisuguste institutsioonide kestvust tihti ohtu seada juba olukord, kus tööprotsesside toimimises tekib kas või pisimgi tõrge.

BSI standard 100-4 on koostatud nõnda, et selle metoodikat saaksid kasutada kõik institutsioonid, sõltumata nende liigist, suurusest ja tegevusvaldkonnast. Standardis kirjeldatakse täielikku, suurtele institutsioonidele suunatud ideaalilähedast juurutamist. Palun arvestage, et kõiki juurutamist käsitlevaid soovitusi ja nende ellurakendamist tuleb alati vaadelda konkreetse institutsiooni kontekstist lähtuvalt. Väiksed ja keskmise suurusega asutused peaksid tööetappe ja ülesandeid rakendama kohandatud kujul.

1.4 Kasutussuunised

Käesolev dokument kirjeldab ja täiendab hädaolukordade halduse juurutamise metoodikat, mis tugineb BSI standardis 100-2 [BSI2] kirjeldatud infoturbe haldussüsteemi juurutamise metoodikale. Rakendades andmeid, mis on kogutud IT-etalonturbe juurutamise raames, on võimalik ära kasutada sünergilisi efekte ja saavutada kulude kokkuhoidu.
Standardi peatükkides 4–9 kirjeldatud metoodikat on soovitatav rakendada järjest, sammhaaval. Erilist tähelepanu soovime juhtida sellele, et hädaolukordade haldust ei tuleks vaadelda kui projekti, vaid kui protsessi, mille edukas juurutamine sõltub ennekõike protsessi erinevate sammude pidevast toimimisest.
Mõistet „institutsioon" kaustakase selles dokumendis neutraalse üldmõistena nii ettevõtete, asutuste kui ka kõikide muude, nii avalike kui ka eraõiguslike organisatsioonide kohta.
Kõik personalialased mõisted ja nimetused kehtivad võrdväärselt nii meeste kui ka naiste kohta. Meessoost sõnavorme on kasutatud üksnes parema loetavuse tagamiseks.

1.5 Kasutatud kirjandus

[BMIKI] Bundesministerium des Innern (BMI), Schutz Kritischer Infrastrukturen - Risiko-und Krisenmanagement, Leitfaden für Unternehmen und Behörden, www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen,templateId=raw,property=publicationFile.pdf/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf, Dez. 2007

[BMIKK] BMI, Bundesministerium des Inneren: Krisenkommunikation - Leitfaden für Behörden und Unternehmen, www.bmi.bund.de, 2008

[BSI1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Managementsysteme für Informationssicherheit (ISMS), BSI standard 100-1, versioon 1.5, juuni 2008, www.bsi.bund.de/

[BSI2] BSI, IT-Grundschutz-Vorgehensweise, BSI standard 100-2, versioon 2.0, juuni 2008, www.bsi.bund.de/

[BSI3] BSI, Risikoanalyse auf der Basis von IT-Grundschutz, BSI standard 100-3, versioon 2.5, juuni 2008, www.bsi.bund.de

[BSIHVK] BSI: Hochverfügbarkeitskompendium, versioon 1.0, ilmunud 1. kvartalis 2009

[BSIKRI] BSI: Schutz Kritischer Infrastrukturen in Deutschland. www.bsi.de/fachthem/kritis/index.htm

[BS259991] British Standards Institute, BS 25999-1:2006 Business Continuity Management,
Part 1: Code of practice, www.thebci.org/standards.htm

[BS259992] British Standards Institute, BS 25999-2:2007, Business Continuity Management, Part 2: Specification, www.thebci.org/standards.htm

[GPG08] Business Continuity Institute, Good Practice Guidelines 2008, www.thebci.org/gpgmoreinfo.htm

[GSK] BSI, IT-Grundschutz-Kataloge - Standard-Sicherheitsmaßnahmen, igal aastal uus, www.bsi.bund.de/gshb

[HB221] Standards Australia, Business Continuity Management, ISBN 0-7337-6250-6, 2004

[INS24001] Standards Institution of Israel, INS 24001:2007, Security and continuity management systems - Requirements and guidance for use, 2007

[ITIL] Office of Government Commerce, IT Infrastructure Library, Service Management - ITIL (IT Infrastructure Library) www.ogc.gov.uk/guidance_itil.asp, Jan. 2008

[ISO20000] International Organization of Standardization (ISO), ISO/IEC 20000, IT Service-Management; bestehend aus ISO/IEC 20000-1:2005, IT Service-Management - Teil 1: Spezifikation für Service Management ISO/IEC 20000-2:2005, IT Service Management - Teil 2: Allgemeine Verfahrensregeln für Service Management

[ISO22399] ISO, ISO/PAS 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management

[ISO27001] ISO, ISO/IEC 27001:2005 Information technology - Security techniques -Information security management systems requirements specification, ISO/IEC JTC1/SC27

[ISO27002] ISO, ISO/IEC 27002:2005 Information technology - Code of practice for information security management, ISO/IEC JTC1/SC27

[NIST34] National Institute of Standards and Technology (NIST), NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, juuni 2002, csrc.nist.gov/publications/nistpubs/

[NFPA1600] National Fire Protection Association, Standard on Disaster/Emergency Management and Business Continuity Programs, 2007, www.nfpa.org

[PAS77] British Standards Institute, PAS 77:2006, IT Service Continuity Management - Code of Practice, www.standardsdirect.org/pas77.htm

[SS540] Singapore Standard, SS 540:2008, Business Continuity Management (BCM), SPRING Singapore, www.spring.gov.sg

2 Hädaolukordade haldus ja IT-etalonturve

2.1 Liigitumine ülejäänud BSI standardite hulka

BSI standardis 100-1 [BSI1] määratletakse infoturbelase haldussüsteemi (ISMS) üldnõudeid, mille hulka kuuluvad ka hädaolukordade halduse üldnõuded. BSI standard 100-2 [BSI2] esitleb IT-etalonturbe meetodit, mille alusel ISMS-süsteemi reaalselt üles ehitada ja töös hoida. Olulisteks teemadeks on turbealase töökorralduse loomine ja selle kaasamine institutsiooni tööprotsessidesse. Selle alla kuulub ka koostöö hädaolukordade haldusega. BSI standard 100-3 [BSI3] käsitleb riskianalüüsi läbiviimise meetodit, mida on kohandatud vastavalt IT-etalonturbe meetodile.

Käesolev BSI standard 100-4 toetub eelnevatele standarditele, kuid kirjeldab eraldiseisvat haldussüsteemi, kuidas tööprotsessidega jätkata ja kuidas hädaolukorda likvideerida. Eesmärgiks on näidata süsteemset lähenemist, millega reageerida võimalikult kiiresti erinevat liiki ja erinevatel põhjustel tekkinud hädaolukordade haldusdele ja kriisidele, mis toovad endaga kaasa tööprotsesside katkemise. See käsitleb enamat kui ainult IT-hädaolukordade haldust (IT-teenuse järjepidevuse haldust) ning seetõttu tohiks seda vaadelda ISMS-i alamvaldkonnana. BSI standard 100-4 kirjeldab, kuidas saab klassikalist IT-etalonturbe meetodit, mida käsitleb BSI standard 100-2 ja riskianalüüsi, mida käsitleb BSI standard 100-3, kasutada alusmaterjalina sobiva hädaolukorraennetuse loomiseks ja võimalikes hädaolukorraolukordades kahjude minimeerimiseks. Dokument juhib tähelepanu asjaolule, et tihe koostöö turvahaldusega on institutsiooni efektiivse hädaolukordade halduse loomisel hädavajalikuks eelduseks. Mida rohkem on tööprotsessid läbi põimunud infotehnoloogia rakendamisega, seda paremini on võimalik ära kasutada ISMS-iga koostöö tegemisest tekkivat sünergiat. Suure kattuvuse tõttu on vägagi soovitatav, et need kaks valdkonda teeksid omavahel tihedat koostööd.

Käesoleva standardiga lisandub uus täiendav tööriist, mis tegeleb IT-etalonturbe meetodi rakendamiseks vajaliku kaitseotstarbe väljaselgitamisega – selleks on tööprotsesside mõjuanalüüs (Business Impact Analysis, BIA). BIA aitab tuvastada kriitilise tähtsusega tööprotsesse ning välja selgitada nii protsesside käideldavusnõudeid kui ka nende ressursivajadusi.

Infotehnoloogilise turvahalduse põhitähelepanu keskendub institutsioonis leiduva info kaitsmisele, hädaolukordade haldus seevastu keskendub kriitilise tähtsusega tööprotsessidele. Andmed liigituvad institutsiooni kaitstavate väärtuste alla (ingl assets), kriitilise tähtsusega tööprotsessid moodustavad aga institutsiooni selgroo. Mõlemat haldussüsteemi iseloomustab kõikehõlmav lähenemine. Mõlema, nii hädaolukordade halduse kui ka IT-turvahalduse, lähtepunktideks on kõikvõimalikud töövaldkonnad.

2.2 Mõisted

Tööprotsesside katkemisel võivad olla väga erinevad põhjused ja ka väga erinevad tagajärjed. Selgitamaks, milliseid kahjujuhtumeid käesoleva hädaolukordade halduse raames käsitletakse, selgitame järgnevalt lühidalt, millises tähenduses on kasutatud mõisteid tõrge, hädaolukord, kriis ja katastroof.

Tõrge
Tõrge on olukord, kus institutsiooni protsessid või ressursid ei toimi nii, nagu nad peaksid toimima. Tekkida võivad kahjud on väiksed. Väikseks kahjuks peetakse kahju, mis on ettevõtte aastase tulemiga või ametiasutuse aastaeelarve mahuga võrreldes kas tühine või mis pärsib tööülesannete täitmist ainult vähesel määral. Tõrkeid kõrvaldatakse igapäevaste tööprotsessidega integreeritud rikkekõrvaldamise protseduuridega. Sellele vaatamata võivad tõrked edasi areneda ka hädaolukordadeks, mistõttu tuleb neid täpselt jälgida, põhjalikult dokumenteerida ja võimalikult kiiresti likvideerida. Nimetatud tegevused ei kuulu siiski mitte hädaolukordade haldusega seotud tööülesannete hulka, vaid nendega peavad tegelema tõrkehalduse eest vastutajad.

Hädaolukord
Hädaolukord on kahju tekitav olukord, kus institutsiooni protsessid või ressursid ei toimi nii, nagu nad peaksid toimima. Vajalike protsesside ja ressursside käideldavust ei õnnestu selleks ette nähtud aja jooksul taastada. Igapäevased tööprotsessid on tugevalt pärsitud. Võimalikke teenindusleppeid (Service Level Agreements, SLA) ei suudeta täita. Tekivad suured kuni väga suured kahjud, mis mõjutavad märkimisväärselt ja vastuvõetamatult suurel määral ettevõtte aasta tulemit või ametiasutuste ülesannete täitmist. Hädaolukordade kõrvaldamiseks igapäevastest tööprotsessidest enam ei piisa. Nende kõrvaldamiseks läheb eraldi tarvis hädaolukordade likvideerimiseks mõeldud töökorraldust.

Kriis
Kriisi all mõistetakse käesolevas dokumendis tavaolukorrast kõrvale kalduvat situatsiooni, mis võib vaatamata ennetavate meetmete rakendamisele tabada ükskõik millist ettevõtet või ametiasutust suvalisel ajal ning mille likvideerimiseks ei piisa tavapärastest meetmetest, mille eest hoolitsevad organisatsiooni struktuur ja töökorraldus. Kriisi likvideerimiseks peab tööle hakkama kriisihaldus. Kriiside likvideerimiseks pole olemas kindlaid protseduuriskeeme, on vaid üldised soovitused ja raamtingimused. Kriisi üheks tüüpiliseks tunnuseks on sündmuse kordumatus.

Hädaolukorrad, mis pärsivad tööprotsesside järjepidevat toimimist, võivad eskaleeruda ja kriisiks muutuda. Sellisel juhul mõistetakse kriisi all teravnenud hädaolukordaolukorda, mis ohustab institutsiooni eksistentsi või inimeste elu ja tervist. Kriis mõjutab peamiselt kas sellest puudutatud ettevõtet või ametiasutust, kuid ei mõjuta ümbritsevat keskkonna ega avalikku elu. Kui mitte tervikuna, siis vähemalt suures osas on seda võimalik likvideerida institutsiooni enda jõududega.

Samas leidub ka üksjagu kriise, mis otseselt igapäevaseid tööprotsesse ei mõjuta. Näideteks on majanduskriisid, juhtimiskriisid, likviidsuskriisid, petturlus, toodete väljapressimine või väärkasutus, inimröövv või pommiähvardus. Käesoleva standardi raames vaadeldavad kriisid moodustavad omaette alagrupi.

Katastroof
Katastroof on suurte kahjudega seotud sündmus, mida pole võimalik ei ajaliselt ega ruumiliselt piirata ning millel on või võib olla laialdane mõju inimestele, väärtushinnangutele ja asjadele. Institutsiooni eksistents ning inimeste elu ja tervis on ohus. Ka avaliku elu toimimine on tugevalt pärsitud. Katastroofi ei ole võimalik likvideerida ainult institutsiooni enda jõududega. Katastroofi geograafiline levik ja selle mõju elanikkonnale eeldavad muuhulgas kindlasti ka seda, et tööle hakkab katastroofiabi. Saksamaal lasub see kohustus liidumaadel ning funktsiooni abistab ja täiendab ka riik. Institutsiooni vaatevinklist võib katastroofi pidada kriisiks, mille likvideerimine eeldab organisatsioonisisese hädaolukorralikvideerimise koostööd väliste abiorganisatsioonidega.

2.3 Hädaolukordade halduse täiendavad standardid

Hädaolukordade halduse teemat käsitletakse paljudes erinevates normides ja riiklikes ning de facto standardites. Järgnevalt lühidalt mõningad näited. Järgnev loetelu ei pretendeeri täielikkusele.

BS 25999-1 / BS 25999-2

[BS259991] British Standards Institute, BS 25999-1:2006 Business Continuity Management, Part 1: Code of Practice kirjeldab hädaolukordade halduse süsteemi juurutamist [BS259991]. Siia alla kuulub muuhulgas ka organisatsiooni struktuur mida nimetatakse järjepidevuse haldusprotsessiks (Continuity Management) ja mis toetub heale tavale (Good Practice).

Nõuded ja töökorralduslike meetmete kontseptsioon. Hädaolukordade halduse detailseid tööetappe või konkreetseid meetmeid siin ei kirjeldata. Siinkohal viidatakse teistele standarditele nagu ISO 27001, ISO 20000 või PAS77.

Briti standard BS 25999-2 Business Continuity Management – Part 2: Specification määratleb punktid, mis on vajalikud Business Continuity Managementi sertifikaadi saamiseks [BS259992].

Tegevuse järjepidevuse haldus (Business Continuity Management) on BS 25999 kohaselt programmiline haldus ja juhtiv element, mille ülesandeks on vastutusalade määratlemine ning mis tagavad tööprotsesside pideva säilimise. BS 25999 toimetsükkel koosneb neljast faasist:

- laialdane arusaamine oma organisatsioonist (läbipaistvus), nt BIA ja riskianalüüsi läbiviimine,
- BCM-i strateegiliste valikute väljatöötamine,
- reageerimismeetmete ja BCM-plaanide väljatöötamine ja juurutamine ning
- BCM-õppuste läbiviimine ja BCM-plaanide ning BCM-meetmete kontrollimine ja edasiarendamine.

Nimetatud nelja faasi peab toetama institutsioonis juurutatava BCM-töökultuuriga.

Hea tava suunised (Good Practice Guidelines, GPG)

Üheks täiendavaks BCM-suuniseks võib pidada hea tava suuniseid (Good Practice Guidelines, GPG), mille on avaldanud Business Continuity Institute (BCI) [GPG08]. BCI asutati aastal 1994. Sellesse kuulub enam kui 85 riiki ning sellel on üle 4000 liikme (teave 2008. aasta veebruarist). Instituudi eesmärgiks on tegevuse järjepidevuse kõrge standardi ja kompetentsi loomine.

Aastal 2002 anti esimest korda välja selle organisatsiooni liikmete koostatud Good Practice Guidelines. Pärast seda on vastavat dokumenti regulaarselt värskendatud ja optimeeritud. GPG on tõlgitud erinevatesse keeltesse. Saksakeelne tõlge pärineb aastast 2005.

BCI GPG 2008 on liigitatud kuude ossa:
- Osa 1: BCM Policy & Programme Management (BCM-i nõuete väljatöötamine ja protsessihaldus),
- Osa 2: Understanding the Organisation (põhjalik arusaam organisatsioonist), Determining BCM Strategy (BCM-i strateegia määratlemine),
- Osa 4: Developing and Implementing BCM Response (reageerimismeetmete väljatöötamine ja juurutamine),
- Osa 5: Exercising, Maintaining & Reviewing BCM arrangements (BCM-meetmete harjutamine, kasutamine ja kontrollimine) ning
- Osa 6: Embedding BCM in the Organisation’s Culture (BCM-i integreerimine organisatsiooni töökultuuriga).

BCI valdkonna hea tava suunised (GPG) on ühed vähesed kvaasi-standardid, mille enam kui 120 lehekülge annavad ka reaalselt rakendatavaid juhiseid, kuidas institutsioonis tegevuse järjepidevuse haldust rakendada.

ISO / PAS 22399
Eelnorm ISO/PAS 22399 Societal security – Guideline for incident preparedness and operational continuity management avaldati aastal 2007 [ISO22399]. Eelnormis „Ühiskonna turvalisus ja kaitse – intsidentideks valmisoleku ja tegevuse järjepidevuse suunised" kirjeldatakse ISO-normidele omases üldistavas vormis, kokku 31 leheküljel, protsessi ja üldpõhimõtteid, millega tegeleb intsidentideks valmisoleku ja tegevuse järjepidevuse haldus (Incident Preparedness and Operational Continuity Management, IPOCM). IPOCM-i tegevustsükkel liigitub kolmeks faasiks:

- Policy (poliitika koostamine),
- Planning (planeerimine),
- Implementation and operation (juurutamine ja rakendamine),
- Performance assessment (suutlikkuse mõõtmine) ning
- Management review (halduse kontrollimine),

ning see sisaldab juba BCM-i toimimistsüklist tuttavaid tööetappe. Mõistet „IPOCM" käsitletakse siinkohal mõiste „BCM" edasiarendusena.

Eelnorm põhineb standarditel NFPA 1600 [NFPA1600], HB 221:2004 [HB221], BS 25999--1:2006 [BS259991], INS 24001:2007 [INS24001] ja jaapani ettekirjutustel. Erilist äramärkimist väärib sihtgrupp. Dokument on suunatud ettevõtetele, kuid erilise tähelepanu all on ka era- ja avalik-õiguslikud organisatsioonid ning juhtimisstruktuurid.

ISO 27001 / ISO 27002
Üha keerukamaks muutuv infotehnoloogia ning aina kasvav nõudlus sertifitseerimise järele on viimastel aastatel tootnud arvukalt juhendeid, standardeid ja infoturbealaseid norme. ISO/IEC 27001 Information technology - Security techniques - Information security management systems requirements specification [ISO27001] on esimene rahvusvaheline infoturbealane standard, mis võimaldab ka sertifitseerimist. ISO/IEC 27001 sisaldab u 10 lk üldisi soovitusi. Normatiivses lisas viidatakse ka turbesoovitustele (Controls), mida kajastab norm ISO/IEC 27002. Praktilisi juurutamisnäpunäiteid lugejale aga ei anta.

Norm ISO/IEC 27002 (eelkäija ISO/IEC 17799) Information technology – Code of practice for information security management [ISO27002] kajastab praktiliste näidete põhjal kokku kogutud kogemusi, protseduure ja meetodeid. Selle eesmärgiks on infoturbealase halduse raamistiku defineerimine. Norm käsitleb seetõttu peamiselt neid vajalikke samme, mida läheb tarvis toimiva turvahalduse ülesehitamiseks ja selle kinnistamiseks organisatoorsetes protsessides. Vastavaid turbealaseid soovitusi kajastatakse põgusalt u 100 leheküljel. Tegevuse järjepidevuse halduse teemat (Business Continuity Management, BCM) käsitleb ISO/IEC 27002 standardi peatükk nr 14. Kokku viiel leheküljel välja toodud BCM-i puudutavad soovitused on väga üldised ning kirjeldavad ennekõike haldamisprotsessi peamisi samme.

NIST SP 800-34
Aastal 2002 NISTI-i (National Institute of Standards and Technology, NIST) poolt avaldatud standard NIST SP 800-34 Contingency Planning Guide for Information Technology Systems on IT-süsteemide hädaolukorraennetamise planeerimist käsitlev suunis [NIST34].

Standard NIST SP 800-34 kirjeldab u 60 leheküljel metoodikat, mille abil luua IT-hädaolukorraennetuse töökorraldust, ning kuidas valida välja ja rakendada IT-hädaolukorra ennetuse ja hädaolukordade likvideerimise meetmeid. Mõningatel juhtudel tuuakse välja ka

konkreetsed lahendused. Lisades on ära toodud vajalike dokumentide plangid, muuhulgas nt Business Impact Analysis ja IT Contingency Plan.

IT-hädaolukordade halduse toimimistsükkel koosneb seitsmest faasist:
- poliitika väljatöötamine
- BIA (Business Impact Analysis) läbiviimine:
- ennetavate meetmete defineerimine (hädaolukorraennetus),
- taastamisstrateegiate väljaarendamine,
- IT-hädaolukorraplaanide väljaarendamine,
- IT-hädaolukorraplaanide koolitus, harjutamine ja testimine ning
- IT-hädaolukorraplaanide värskendamine.

Sihtgrupiks on peamiselt USA ametiasutused. Sellele vaatamata on suunis siiski kasutatav igat liiki ning erineva suurusega organisatsioonides.

PAS 77 / BS 25777

Public Available Specification 77:2006 IT Service Continuity Management - Code of Practice standardi väljaandjaks on British Standards Institution [PAS77]. Standard kirjeldab põhimõtteid ja meetodeid, mille abil saab üles ehitada ja rakendada IT-teenuse järjepidevuse haldust (IT Service Continuity Managements). Sellele eelstandardile pääseb küll avalikult ligi, kuid selle eest tuleb maksta. PAS 77-t võib vaadelda kui BS 25999 täiendavat osa IT-teenuste hädaolukorraennetuse planeerimise valdkonnas. Hetkel arendatakse seda edasi, ning värskendus peaks valmima dokumendina BS 25777 Code of practice for information and communications technology continuity. Esmaeksemplar, 38 lk, anti 2008. a septembris väliste kommentaaride lisamise eesmärgil vabaks ning see on tasu eest kättesaadav.

Selle spetsifikatsiooni sihtgrupiks on IT-teenuste järjepidevuse (IT Service Continuity) ülesehituse, rakendamise ja säilimise eest vastutavad töötajad. Eesmärgiks on IT-hädaolukorraennetuse juurutamine kriitilise tähtsusega IT-teenuste tarbeks. Vastavad meetmed ja plaanid peavad minimeerima IT-käituse katkemisohu ning kui mõni IT-teenus on rivist välja langenud, tagama funktsioonide kiire taastamise.

ISO / IEC 24762

2008. a alguses avaldatud norm ISO/IEC 24762 Information technology – Security techniques – Guidelines for information and communication technology disaster recovery services käsitleb info- ja kommunikatsioonitehnoloogia taaskäivitamisteenuste nõudeid. Norm on suunatud nii sisemistele kui ka välistele teenusepakkujatele, kelle valdkonnaks on ICT (Information and Communication Technology) DR (Disaster Recovery) Services ning selles kirjeldatakse nõudeid DR-teenuste juurutamisele, käitamisele, seirele ja teenuse säilimisele. ICT-DR-Services on vaadeldav Business Continuity Managementi ühe osana.

ITIL

ITIL (IT Infrastructure Library) on dokument, mida annab välja, täiendab ja arendab briti valitsusasutus Office of Government Commerce (OGC). Praegu kehtiv versioon, ITIL V3, ilmus aastal 2007. Sellest on kujunenud ülemaailmselt aktsepteeritud de facto standard, mis käsitleb olulisemate IT-juhtimisprotsesside loomist, rakendamist ja haldamist. Tegu on protseduure kajastava andmeteegiga, kuhu on kogutud hea tava publikatsioonid, mis käsitlevad IT-teenuste planeerimis- ja juhtimismeetodeid.

IT-teenuse haldus (IT Service Management) on keskne töökorralduslik instrument, mis aitab IT kasutamist vastavalt tööprotsesside vajadustele optimeerida ja võimaldab IT-teenuste kasutamist lähtuvalt klientide vajadustest juhtida. Vastavad teenusehalduse protsessid moodustavadki ITIL-i tuuma.

IT Service Continuity toimimistsükkel koosneb ITIL-i järgi neljast faasist:
- protsessi algatamine: poliitikate (Policy) ja ulatuse / kehtivusala / IT-koosluse (Scopes) määratlemine,

- vajadused ja strateegia: BIA (Business Impact Analysis), riskianalüüs ja järjepidevusstrateegia,
- juurutamine: järjepidevusplaanide, taastamisplaanide ja testimisstrateegiate väljatöötamine,
- operatiivne haldus: koolitamine ja teadlikkuse tõstmine, revisjonid, testimised ja muudatuste haldus (Change Management).

ITIL-i teadmised on saadaval u 40 ingliskeelse publikatsiooni näol [ITIL]. ITIL-i kaks peamist koostisosa, IT-teenuste tugi ja IT-teenuste pakkumine (Service Support, Service Delivery) on lisaks olemas ka saksakeelse kokkuvõttena, mida on samuti täiendatud.

ISO/IEC 20000

Standard ISO/IEC 20000 IT Service Management tugineb briti standardile BS 15000 ning võimaldab IT-teenuste haldust (IT Service Management) sertifitseerida. Standard koosneb kahest osast. ISO 20000 Part 1 defineerib sertifitseerimiseks hädavajalikke miinimumnõudeid ning sisaldab ka täiendavaid nõudeid, suuniseid ja soovitusi. Part 2 sisaldab haldussüsteemi ülesehitamist ja tööshoidmist puudutavat head tava [ISO2000]. Juurutamise põhimõtted saab selleks otstarbeks tuletada ITIL-i hea tava valdkonnast (ITIL Best Practices). IT-hädaolukorraennetuse seiskohast oluline lõik 6.3 Service continuity and availability management määratleb ühtekokku kaheksat kontrollielementi, mida on tarvis ISO 20000 sertifikaadi saamiseks täita. Need on järgmised:

1. Business plan requirements (tegevuse planeerimise nõuded),
2. Annual reviews (aastased kontrollid),
3. Re-testing plans (järelkontrollide plaanid),
4. Impact of changes (muudatustega kaasnevad mõjud),
5. Unplanned non-availability (plaaniväline käideldavuse kadu),
6. Availability of resources (ressursside käideldavus),
7. Business needs (tegevusvaldkondade nõuded),
8. Recording tests (kontrollide dokumenteerimine).

3 Hädaolukordade halduse protsess

Ettevõtete ja ametiasutuste hädaolukordade haldus on keeruline protsess, mis hõlmab endas nii hädaolukorraennetust, hädaolukordade likvideerimist kui ka hädaolukorrajärgseid tegevusi. Sellise protsessi juurutamiseks ja tööshoidmiseks läheb ilmtingimata tarvis efektiivset haldussüsteemi.

3.1 Ülevaade

Hädaolukordade halduse loomiseks on vaja süsteemset metoodikat. Hädaolukordade halduse protsess koosneb järgmistest faasidest: hädaolukordade halduse algatamine, kontseptsiooni loomine, hädaolukorraennetuse kontseptsiooni rakendamine, hädaolukorade likvideerimine, testimine ja harjutamine ning hädaolukordade haldusprotsessi tööshoidmine ja pidev täiendamine.

-► Hädaolukordade halduse algatamine
▼
-► Kontseptsioon
▼
Hädaolukorraennetuse kontseptsiooni rakendamine
▼
Hädaolukorra likvideerimine
▼
Testid ja harjutamine
▼
Hädaolukordade haldusprotsessi toimimise tagamine ja pidev parandamine

Joonis 1. Hädaolukordade halduse protsess

Enne seda, kui institutsioonis asutakse juurutama hädaolukordade haldust, tuleb kõigepealt paika panna vastavad raamtingimused. Esmalt tuleks koostada hädaolukordade halduse poliitika, mille algatamine, kaasaarendamine ja heakskiitmine lasub juhtkonna vastutusel. Lisaks tuleb hädaolukordade halduse toimimiseks luua töökorralduslikud eeltingimused. Siia alla kuulub inimeste tööülesannete ja vastutusalade määramine ning juhatuse või juhtkonna poolt piisavate materiaalsete vahendite eraldamine. Hädaolukordade halduse edukus sõltub suuresti selle edukast integreerimisest ametiasutuse või ettevõtte olemasoleva töökultuuriga. Selle saavutamiseks tuleb töötajad protsessi kaasata ja nad oma tööülesanneteks ette valmistada, viies läbi teadlikkust tõstvaid ja oskusi vahendavaid koolitusi.

Hädaolukordade halduse kontseptsiooni aluspõhja moodustavad andmed, mis on kogutud nn tööprotsesside mõjuanalüüsi (Business Impact Analysis, BIA) raames. BIA raames selgitatakse välja institutsiooni jaoks kriitilise tähtsusega tööprotsessid ja määratakse kindlaks nende taaskäivitamise prioriteedid. Lisaks kogutakse BIA käigus andmeid selle kohta, milliseid ressursse läheb protsessi jaoks tarvis ning millised on hädaolukorrakäituse miinimumnõuded.

Analüüsi käigus tuvastatud kriitilise tähtsusega protsesside ja ressursside kohta viiakse läbi riskianalüüs. Selle käigus vastatakse küsimusele: „mis ohustavad meie protsesse ja ressursse?”. Juhtudel, kus vastavad andmed on juba mõne muu haldussüsteemiga kokku kogutud, võib riskianalüüs ära jääda.

BIA ja riskianalüüsi põhjal kogutud andmete baasil töötatakse välja erinevad strateegiavõimalused, mille hulgast saab välja valida sobivad järjepidevusstrateegiad. See moodustab raamistiku, mille põhjal saab välja valida ennetavad meetmed ja määratleda nendega seotud investeeringud. Seejärel määratakse kindlaks ja rakendatakse ellu hädaolukorraennetuse meetmed (hädaolukorraennetuse kontseptsioon). Siia alla kuulub ka hädaolukorrakäsiraamatu väljatöötamine, millest saab baasmaterjal ja abivahend hädaolukordade likvideerimisel.

Hädaolukordade halduse toimimise tagamiseks ja selle pideva täiendamise tagamiseks tuleb erinevatesse hädaolukorradokumentidesse kirja pandud meetodeid ja protseduure testida ja harjutada, samuti tuleb analüüsida hädaolukordade likvideerimisi ning läbi viia muid täiendavaid regulaarseid kontrolle. Nimetatud tegevuste käigus välja selgitatud vajadused kas muudatuste või kohanduste järele peavad leidma tee protseduuride ja plaanide pidevasse kohandamisse, parandamisse ja värskendamisse. Aina korduva hädaolukorraennetuslike meetmete ja hädaolukorraplaanide ümbertöötamisega peab hoolitsema selle eest, et hädaolukordade haldus oleks alati kõige optimaalsemas seisus.

3.2 Dokumentatsioon

Hädaolukordade haldusse puutuvates protsesside raames töötatakse välja erinevaid kontseptsioone, arendatakse välja mitmeid kontrolli- ja testiaruandeid ning luuakse veel palju muid institutsiooni hädaolukordade haldust kajastavaid dokumente. Tulevikus tehtavaid vigu on võimalik vältida vaid juhul, kui vastu võetud otsuste ja sooritatud tegevuste mõistmine ning kitsaskohtade tuvastamine tugineb korralikul dokumentatsioonil.

Hädaolukorras kiire ja efektiivne tegutsemine sõltub suuresti olemasolevast dokumentatsioonist. Lisaks sellele, et dokumendid peavad olema kvaliteetsed ja kajastama kõige värskemat infot, on märkimisväärne roll ka nende kättesaadavusel. Hädaolukordade likvideerimisega tegelevatel töötajatel peab tööks vajalikele dokumentidele olema kiire juurdepääs.

Koostatavate dokumentide näited:
- hädaolukordade halduse poliitika,
- hädaolukorraennetuse kontseptsioon koos BIA ja riskianalüüsi aruannetega,

- hädaolukorrakäsiraamat kõige värskemate kontaktandmetega,
- harjutuste käsiraamat, harjutuste plaan, harjutuste kontseptsioonid ja protokollid
- koolituse ja teadlikkuse tõstmise kontseptsioon,
- likvideeritud hädaolukordade analüüsid,
- revisjonide aruanded
- muud aruanded ning
- juhtkonnale mõeldud otsuselangetamismallid

3.2.1 Hädaolukordade halduse dokumentidele kehtestatud minimaalsed märgistusnõuded

Dokumendid, mida hädaolukordade halduse raames koostatakse, muudetakse ja hallatakse, peavad olema sisukad ja iga sihtgrupi jaoks arusaadavad. Dokumentide struktuur võiks olla mõistlikkuse piires võimalikult ühesugune. See lihtsustab dokumentide kasutamist ja aitab kaasa nende kiiremale mõistmisele. Dokumendid peavad olema märgistatud selliselt, et neid oleks vajaduse korral võimalik kiiresti üles leida ja liigitada. Selleks peab dokumentidel kajastuma vähemalt järgnev info:

- üheselt mõistetav nimi (sisu edasiandev pealkiri),
- koostaja / autor / dokumendi omanik,
- dokumendikoostaja funktsioon,
- versiooni number,
- viimane täiendus, järgmine planeeritud täiendus,
- heaks kiidetud kuupäeval / kelle poolt,
- liigitus, (konfidentsiaalne info tuleb liigitada klassidesse, vastavalt tähistada ning dokumente tuleb hoida turvaliselt) ning
- volitatud töörollid (asjasse pühendatud ringkond).

Täiendavalt võib kajastada ka järgnevat infot:
- viited allikatele,
- säilitamiskohustus ja
- ülevaade tehtud muudatustest.

3.2.2 Detailsuse aste

Dokumentides kajastuva info detailsuse suhtes kehtib põhimõte: vastavalt eesmärgile ja vajadusele. Strateegiadokumendid (nagu poliitika) peaksid olema lühidad ja tabavad, kuid samas sisutihedad. Kontseptsiooni koostamise käigus tekkivate dokumentide andmed peaksid olema varasematest detailsemad, et oleks võimalik nende põhjal langetatud otsuseid mõista. Kõik otsused nagu ka andmed, mille põhjal otsused vastu võeti, tuleb dokumenteerida.

Kõikidele dokumentidele, eriti aga nendele dokumentidele, mida kasutatakse hädaolukordade likvideerimisel, kehtib nõue, et need peavad olema selges ja arusaadavas keeles. Andmete detailsuse aste tuleks valida selline, et dokumendid oleksid arusaadavad ka valdkonnas pädevale kolmandale osapoolele. Selles valdkonnas pole soovitatav koostada põhjalikke tegutsemisjuhiseid võhikutele, kuna eesmärgiks on kiire tegutsemine. Tihti piisab paljude valdkondade jaoks kontrollnimekirjadest. Need aitavad luua kiire ülevaate, vähendavad unustamisvõimalusi ja aitavad kinni pidada üksikute tööetappide kindlast järjekorrast.

3.2.3 Muudatuste haldus

Muudatuste halduse jaoks on elementaarne, et need peavad kajastama kõige värskemaid andmeid (nt kontaktandmeid, keda hädaolukorrast teavitada, kes tegeleb eskalatsiooniga, ja kontaktisikud). Selleks, et kõikide hädaolukordade haldust käsitlevate dokumentide regulaarne värskendamine oleks tagatud, on soovitatav võtta kasutusele mõni muudatuste haldamise protseduur, mis võimaldaks kõik vajalikud muudatused kokku koguda ning neid

analüüsida, kasutusse anda ja mõista. Selle tarbeks tuleb kõikide dokumentide kohta luua muudatuste haldust reguleerivad selged ettekirjutused. Lisaks peaks see protseduur määratlema selle, mil moel on kasutajatel võimalik muudatusettepanekuid edastada ning kuidas neid muudatusettepanekuid hinnatakse ja vajadusel üle võetakse. Hädaolukordade halduse muudatuste haldus tuleb integreerida üleinstitutsioonilise muudatuste haldusega.

Dokumentide värskendamisele tuleb kehtestada ajalised intervallid. Enamasti piisab dokumentide puhul sellest, kui nende ajakohasust kontrollitakse kord aastas. Seevastu dokumentide puhul, mis sisaldavad vajalike isikute kontaktandmeid, tuleks andmete õigsust kontrollida vähemalt kord kvartalis, veel parem, kui kord kuus. Selleks tuleb teha koostööd organisatsiooni personaliosakonnaga. Kuna tänapäeva tööprotsessid võivad kiiresti muutuda, on soovitatav, et BIA-t (Business Impact Analysis) töötataks läbi ja värskendataks iga poole aasta tagant.

Lisaks regulaarsetele kontrollidele peaks asjakohaste dokumentide muutmise kohustus kehtima ka veel juhtudel, kus muudetakse raamtingimusi, ettevõtluse valdkonda, ülesandeid või strateegiaid. Tuleb tagada, et ka väiksed, kuid siiski olulised muudatused tähendaksid asjast puudutatud dokumentide muutmist. Siia kuulub kindlasti nt hädaolukorratöökohti puudutav info nagu muutused personalis, hädaolukordade haldusega tegelevate isikute kontaktandmed, töötajate kolimised ühest tööruumist teise, tööruumide sisustuse ja IT muutused.

Vastavad mehhanismid, mis eeldavad muudatuste halduse rakendumist, tuleb integreerida organisatsiooni muude siseprotsessidega (nt personalijuhtimisega, majahaldusega, inventariseerimisega). Hädaolukorraametniku tööks on juhtimine. Dokumentide värskendamise ja dokumentidele kehtivate muutmisnõuete järgimise eest vastutab dokumentide omanik.

3.2.4 Dokumenteerimiseks kasutatav meedium

Hädaolukordade halduse dokumendid ei pea alati ilmtingimata paberkandjal olema. Dokumenteerimiseks võib kasutada ka tarkvaratööriistu, internetil põhinevaid tehnoloogiaid, sülearvuteid või ka pihuarvuteid. Viimased võimaldavad kõiki andmeid salvestada ja neid saab kasutada erinevates asukohtades.

Hädaolukorrakäsiraamatu ja kõikide teiste hädaolukordade likvideerimiseks vajalike dokumentide puhul on soovitatav hoida neid nii, et need oleksid kiiresti käepärast, kas väljatrükkidena ja/või elektroonilisel kujul, lihtsasti kasutatavates andmeformaatides (nt PDF- või HTML-failidena mälupulga peal koos vastava kuvamisprogrammiga). Valitud lahendus peab tagama, et hädaolukorras oleksid dokumendid kättesaadavad ja seda nii elektrikatkestuse kui ka teiste riskide puhul, mis võivad dokumente kasutuskõlbmatuks muuta, andmeid hävitada või juurdepääsu andmetele tõkestada. Seetõttu on soovitatav, et dokumentide varukoopiaid hoitaks kuskil eraldi asukohas. Kriisiolukordades tuleb otsuseid langetada väga kiiresti, mis tähendab, et ei ole aega dokumente serverilt või sülearvutist otsima hakata ega neile kuhugi kaugele järele minna. Täiendavat stressi ja tegelikust ülesandest kõrvalekaldumist võib tekitada ka olukord, kus hädaolukorradokumente hallatakse tarkvaratööriistadega, mida kasutatakse kas väga harva või mida pole kunagi kasutatud. Stressisituatsioonides peaks kasutajal olema täiendav kindlus.

Seetõttu tuleks dokumenteerimiseks kasutatava meediumi valikul lähtuda vajadusest (nt lugemine või dokumenteerimine), faasist (hädaolukorraennetus või hädaolukordade likvideerimine) või mõnest etapiülesandest. Valikupõhimõtetena tuleks arvestada veel ka dokumentidega ümberkäivaid inimesi ja nende oskusi erinevaid meediumeid kasutada. Ühed inimesed eelistavad võib-olla paberdokumente, teised jällegi ei suuda elu ilma elektrooniliste dokumentideta ja ilma nende otsingu- või filtreerimisfunktsioonideta üldse ettegi kujutada.

3.3 Infoturve ja andmekaitse

Kuna hädaolukordade halduse dokumendid kajastavad ka isikuandmeid ja konfidentsiaalseid andmeid institutsiooni kohta, tuleb hoolitseda nii infoturbe kui ka andmekaitse eest. Lisaks käideldavusele on ilmtingimata tarvis tagada ka dokumentide tervikluse, eriti nende konfidentsiaalsuse säilimine. Hädaolukordade halduse dokumendid tuleb vastavalt nende konfidentsiaalsusele klassidesse liigitada, vastavalt märgistada ning asjakohaste meetmetega kaitsta.

Dokumentides tuleb ära märkida nende volitatud kasutajad. Ligipääs dokumentidele peaks piirduma nende töötajatega, kes vastavaid dokumente oma töös reaalselt vajavad (piisava informeerituse põhimõte). Seetõttu on soovitatav dokumendid mõistlikkuse piires moodulitesse jaotada. See võimaldab levitada teavet selle adressaatide alusel. Institutsioonis peaks olema ülevaade sellest, kuidas on erinevad dokumendid klassidesse jaotatud ja mis liiki need on (nt paberdokumendid või CD-d), samuti peaks olema korrektne ja täielik ülevaade nende muutmise, hävitamise ja kehtetuks tunnistamise kohta.

Hädaolukorrakäsiraamatule ja kõikidele teistele hädaolukordade likvideerimist käsitlevatele dokumentidele kehtivad väga kõrged käideldavusnõuded (vt lisaks ptk 3.2.4), kuid see ei tähenda, et konfidentsiaalsuse arvelt võiks teha järeleandmisi. Näiteks USB-mälupulkade kasutamine salvestusvahendina hädaolukorraplaanide jaoks on hea valik, kuna garanteerib kiire käideldavuse, kuid ilma täiendavate turvameetmeteta, mis suudaksid tagada konfidentsiaalsust, pole nende kasutamine soovitatav. Tuleb valida sellised meetmed, mis tagavad konfidentsiaalsuse, ilma et käideldavus seetõttu hädaolukorra- või kriisolukorras kannataks. Juurdepääsu kaitsmiseks ja krüpteerimiseks võib kasutada nii spetsiaalset riistvara (nt biomeetrilisi süsteeme) kui ka tarkvaralisi lahendusi, kuid peamine on siiski eelnev kontroll, kas vastavad lahendused on hädaolukordades kasutatavad või mitte. Hädaolukorras võib näiteks vajaliku, interneti või intraneti kaudu ligipääsetava PKI (Public Key infrastruktuuri) väljalangemine kujuneda suureks probleemiks, samuti võib stressisituatsioonis tekkida volitatud kasutaja volituste ekslik mittetunnistamine (False Rejection), kuna sõrmejäljelugeja ei saa higise näpu lugemisega hakkama.

4 Hädaolukordade halduspротsessi algatamine

Hädaolukordade halduse ülim eesmärk on tagada kriitilise tähtsusega tööprotsesside säilimine ning hoida institutsiooni võimalike kahjujuhtumite mõjud võimalikult väikestena. Selle saavutamiseks tuleb vastu võtta strateegilisi otsuseid, luua töökorralduslikud struktuurid ja rakendada erinevaid meetmeid. Algatamisfaasi esimesteks sammudeks on vastutuse võtmine ametiasutuse või ettevõtte juhtkonna poolt ja hädaolukordade halduse üldiste põhimõtete väljatöötamine.

4.1 Vastutuse võtmine juhtkonnas

Valdkonna tõsidus ja langetatavate otsuste laiaulatuslikud tagajärjed teevad hädaolukordade haldusest protsessi, mida peab algatama, juhtima ja kontrollima juhtkonna kõige kõrgem tasand. Seetõttu on väga oluline, et juhtkond tegeleks aktiivselt institutsiooni jaoks hädavajaliku hädaolukordade halduse temaatikaga. Juhtkonda tuleb teavitada sellest, miks peab institutsioonis hädaolukordade halduse juurutama.

Hädaolukordade halduse, nagu ka infoturbehalduse [BSI2] eest., vastutab institutsiooni juhtkonna kõige kõrgem tasand. Juhtkond vastutab selle eest, et kõik tegevusvaldkonnad funktsioneeriksid eesmärgikohaselt ja korralikult, et suudetaks tuvastada ja vähendada riske ning minimeerida institutsioonis tekkida võivate kahjujuhtumite tagajärgede ulatust.

Mõni juhtkonna kõige kõrgema tasandi liige tuleks nimetada hädaolukordade halduse protsessi juhiks, kellel lasuks täielik vastutus. See juhatuse liige peab tagama, et institutsioonis juurutatakse hädaolukordade haldus ning et poliitikas sõnastatud ettekirjutusi järgitakse. Siinkohal tuleb arvestada organisatsiooni tüübist ja tegevusvaldkonnast, samuti seadustest tingitud eripärasid.

Hädaolukordade halduse ülesanne, st hädaolukordade halduse ülesehitamine ja selle tööshoidmine, delegeeritakse juhatuse poolt reeglina mõnele hädaolukorraametnikule. Sellele vaatamata on jätkuvalt vajalik, et juhatus oleks aktiivselt kaasatud nii kontseptsioonide loomisse kui ka hädaolukordade likvideerimisse, kuna juhatus peab strateegiliste otsuste langetamisega tagama, et ükski vastuvõetamatult suur risk ei jääks tähelepanuta ja et ressursse investeeritaks õigetesse valdkondadesse. Isegi siis, kui hädaolukordade halduse protsesside raames delegeeritakse erinevaid ülesandeid edasi kas kindlatele isikutele või organisatsiooni allaüksustele, jääb delegeerimatu koguvastutus siiski institutsiooni juhatuse kanda.

Juhatus peab hoolitsema selle eest, et hädaolukordade halduse käsutusse antakse piisavad ressursid (personal, aeg, finantsid). Juhatus vastutab selle eest, et hädaolukordade halduse erinevad aspektid saaksid integreeritud kõikide oluliste tööprotsesside- ja protseduuridega ning pakub abi hädaolukordade halduse erinevatele organisatsioonilistele allüksustele.

4.2 Hädaolukordade halduspротsessi kontseptsiooni loomine ja planeerimine

Avarihalduse protsessi juurutamine on projekt, mis eeldab planeerimist. Kõikvõimalike kulutuste väljaselgitamiseks ning ajakulu ja ressursside planeerimiseks on tarvis sõnastada hädaolukordade halduse eesmärgid, määratleda kehtivusala, välja töötada raamtingimised ja strateegia, millega püstitatud eesmärke saavutada.

4.2.1 Hädaolukordade halduse defineerimine

Institutsiooni juhatus peab määratlema, mida mõistetakse hädaolukordade halduse all ning millised on hädaolukordade halduse ülesanded ja kompetentsid. Kuna institutsioonis on reeglina juba juurutatud mitmeid haldussüsteeme nagu IT-haldus, infoturbehaldus,

majahaldus, kvaliteedihaldus või riskihaldus, tuleks välja selgitada, millised on nende valdkondade kokkupuutepunktid või kattuvused hädaolukordade haldusega. Erinevate valdkondade vastavad kokkupuutepunktid, kompetentsid ning võimalusel ka õigused ja kohustused tuleb üheselt määratleda ja dokumenteerida.

4.2.2 Kehtivusala määratlemine

Hädaolukordade halduse kehtivusala tuleb üheselt määratleda. Kehtivusalaks võib olla terve institutsioon koos oma kõikide erinevate asukohtadega või hoopis üksikud valikulised asukohad või erandjuhtudel koguni ainult mõned tegevusvaldkonnad. Kehtivusala peaks olema suletud, kuid mitte liiga kitsalt piiritletud, ja peaks sisaldama väärtuseid loovaid tööprotseduure või olulisi erialaseid ülesandeid, olulisemaid ressursse ning vajalikke toetavaid tööprotseduure. Kehtivusala määratlus võib vajadusel sisaldada võimalikke hädaolukordade haldusele kehtestatud piiranguid ja selle piire. Soovi korral võib rõhutada olulisi tööprotsesse või tööülesandeid, mis jäävad kehtivusala piiridesse.

Kuna hädaolukordade halduse eesmärgiks on institutsiooni ellujäämisvõime tagamine ja stabiliseerimine, tuleks püüelda selle poole, et hädaolukordade haldus käsitleks tervet institutsiooni. Ainult sel moel on võimalik tagada, et institutsiooni imidž ja väärtuseid loovad tegevused ja seega ka oluliste huvigruppide huvid on tõhusalt kaitstud.

4.2.3 Seadustest tulenevad ja muud ettekirjutused

Hädaolukordade halduse tegevuse jaoks tuleb välja selgitada kõik olulised seadused, direktiivid ja ettekirjutused. Institutsiooni suhtes kehtivate nõuete väljaselgitamiseks tuleks esmalt alati läbi töötada kehtivad seadused. Iga tegevusvaldkonna kohta leidub reeglina palju spetsiifilisi ettekirjutusi ja standardeid, mida tuleb võib-olla arvestada. Milliseid täpselt, see sõltub muuhulgas institutsiooni õiguslikust vormist, tegevusvaldkonnast ja tööprotsesside spetsiifikast. Hädaolukordade haldusele kehtivad seaduslikud ettekirjutused võivad tekkida nt dokumentidest nagu Sarbanes-Oxley Act, ettevõtluse kontrolli ja läbipaistvuse seadus (KonTraG), Baseli omakapitalikokkulepped (Basel II), aktsiaseadus (AktG), posti ja telekommunikatsiooni kaitse seadus (PTSG), börsiseadus (BörsG), töökaitseseadus (ArbSchG), rikkejuhtumite määrus (12. BImSchV – StörfallV), ohtlike ainete käitlemise määrus (GefStoffV) või tööturvalisuse määrus (BetrSichV).

4.2.4 Hädaolukordade haldusele seatavad eesmärgid ja nõuded

Institutsiooni juhtkond peab määratlema strateegilised eesmärgid, mida on tarvis hädaolukordade halduse ülesehitamisel ja tööshoidmisel järgida. Hädaolukordade halduse strateegia või lühidalt hädaolukordastrateegia alla kuulub muuhulgas kõik järgnev:
- määratlused, milliseid ärilisi eesmärke on tarvis kaitsta,
- millised on kõige olulisemad võimalikud kahjustsenaariumid,
- milliseid katkestusi tootmises peetakse jätkusuutlikkust ohustavaks,
- milline on valmidus riskida (riskivalmidus) või kui kõrge on ettevõtte või ametiasutuse vastuvõtlikkus riskide suhtes,
- millisel viisil ja millises suurusjärgus tuleks midagi riskide vastu ette võtta ja
- milline on hädaolukordadega tegelemise esmane eesmärk.

Hädaolukorrastrateegiasse võib nt kirja panna, et esmatähtsaks peetakse olemasolevate tellimuste täitmist ja uusi tegevusalasid juurde ei lisandu, et kõik ärilised protsessid peavad töötama vähemalt 50-protsendilise võimsusel või läbilaskel või et hädaolukordadega tegelemise peamiseks eesmärgiks on vältida kahju levimist, eriti selliselt, et hädaolukord ei kanduks üle koostööpartneritele, ning et selline tegevus on kõrgema prioriteediga kui tootmise võimalikult kiire taaskäivitamine.

Vastavad hädaolukordade haldusele kehtivad nõuded saab tuletada kas tootmis- või tööprotsessidest, seadusega ette antud raamtingimustest ja ennekõike muidugi ettevõtte ja ametiasutuse ärilistest ja programmilistest eesmärkidest. Kasu võib olla ka nn huvigruppide analüüsist (Stakeholder Analysis). Analüüsi raames selgitatakse välja peamised huvigrupid (Key Stakeholders), kellel võib olla huvi ja on seetõttu ka võimalus institutsiooni hädaolukordade haldust mõjutada, ükskõik, kas tegu on isikliku huvi, kolmandate isikute huvide esindamise või ettevõtte käekäigu eest seismisega. Võimalike huvigruppidena võib vaadelda nt osanikke, töötajaid ja nende lähikondlasi, investoreid, kliente, tarnijaid, aga kindlustajaid, järelvalveameteid, valdkonna erialaliidesed ja seadusandjaid.

4.2.5 Planeerimispõhimõte

Hädaolukordade halduse protsessi loomiseks ja ellurakendamiseks kuluvate tööde mahtu ei tohiks alahinnata. Ülevaate ja motivatsiooni säilitamiseks tuleks valida reaalsed eesmärgid ning kogu ülesehitamise protsess ehk mitmesse etappi jagada. Soovitatav on määratleda mõistlikud vahe-eesmärgid ja saavutatavad verstapostid. Nii näiteks võiks esimeses etapis keskenduda üksnes peamistele protsessidele ja vältida nende erinevate sammude liiga detailset väljatöötamist. Pärast seda, kui hädaolukordade halduse esmane tase on saavutatud, peaks hädaolukorraprotsessi raames aset leidma selle pidev täiendamine ja taseme tõstmine, parandades erinevaid meetodeid, laienedes täiendavatele tegevusvaldkondadele ja tehes protsessietappe üha detailsemaks.

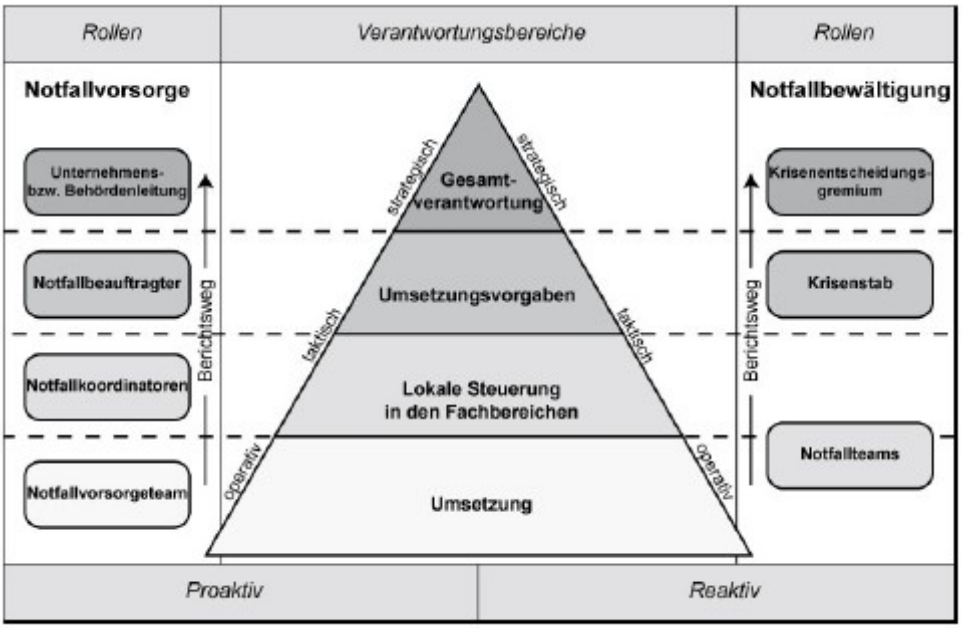
4.3 Töökorralduslike eelduste loomine

Hädaolukordade haldust võib jagada hädaolukorraennetuseks ja hädaolukorra likvideerimiseks. Hädaolukorraennetuse tegevus on oma olemuselt proaktiivne, hädaolukordade likvideerimine seevastu reageeriv. Viimane võetakse ette hädaolukorraolukorra tekkides.

Hädaolukordade halduses on võimalik eristada kolme vastusala:
- strateegiline valdkond (anglosaksi keelekasutuses tuntud ka kui Gold Team),
- taktikaline valdkond (Silver Team) ja
- operatiivne valdkond (Bronze Team).

Strateegiavaldkonna kanda on koguvastutus tegutsemise ja planeerimise eest, mille eesmärgiks on institutsiooni eesmärkide saavutamine, ning seetõttu peab sellega tegelema juhtkond. Taktiline vastusala hõlmab strateegiliste ettekirjutuste ellurakendamist organisatsiooni erinevates allüksustes Operatiivne vastutusala tegeleb strateegilise ja taktikalise tasandi loodud ettekirjutuste ellurakendamisega.

Allolev joonis annab ülevaate kolme vastutusala rollidest ja nende seostest hädaolukorraennetuse ja hädaolukordade likvideerimise valdkonnaga. Järgmises kahes alapeatükis sisalduvad kirjeldused käsitlevad nende ülesandeid, vastutusalasid, kompetentse ja volitusi.



Joonis 2. »Töörollid ja vastutusalad
Rollen – rollid; Verantwortungsbereiche – vastutusalad, Notfallvorsorge – hädaolukorraennetus, Notfallbewältigung – hädaolukordade likvideerimine; Unternehmens bzw. Behördenleitung – ettevõtte või ametiasutuse juhtkond; Notfallbeauftragter – hädaolukorraametnik, Notfallkoordinatoren – hädaolukorrakoordinaatorid; Notfallvorsorgeteam – hädaolukorraennetuse meeskond; Berichtsweg – aruandluse suund: Proaktiv – ennetav; Reaktiv – reageeriv; Gesamtverantwortung – koguvastutus; Umsetzungsvorgaben – rakendamisalased ettekirjutused; Lokale Steuerung in den Fachbereichen – lokaalne juhtimine erialastes osakondades; Umsetzung – rakendamine

Kõiki kirjeldatud töörolle ei lähe kõikides institutsioonides ilmtingimata tarvis. Vajadus sõltub organisatsiooni suurusest, selle loogilisest struktuurist ja organisatsiooni allüksuste omavahelisest geograafilisest kaugusest. Valik ja kaasatavate töötajate hulk tuleb kohandada vajadustega. Valitud struktuur tuleb üheselt mõistetavalt dokumenteerida. Põhitöö kõrvalt mitme rolli täitmine on võimalik tingimusel, et vastaval töötajal on olemas vajalik kvalifikatsioon ja et tal on nende ülesannete täitmiseks kasutada piisav ajaline ressurss. Sugugi mitte kõik töörollid ei eelda täiskoormusega töökohta, vaid neid saab täita ka täiendavate ülesannetena, eriti väikestes ja keskmise suurusega institutsioonides.

4.3.1 Hädaolukordade halduse töökorralduse rollijaotused

Ettevõtte või ametkonna juhtkond
Ettevõtte või ametkonna juhtkond vastutab üleinstitutsioonilise hädaolukordade halduse tagamise eest. Juhtkond määratleb, milline on hädaolukordade halduse tähendus institutsioonile, määrab ära selle ellurakendamise strateegilise suuna ning eraldab majanduslikest kaalutlustest lähtuvalt vajalikud finantsid ja personaliressursi. Institutsiooni juhtkond nimetab ametisse hädaolukorraametniku ja annab talle volitused, mis lubavad tal hakata tegelema hädaolukordade haldusprotsessi planeerimise ja koordineerimisega.

Hädaolukorraametnik
Hädaolukorraametnik juhib kõiki hädaolukorraennetusega seotud protsesse ja lööb nendega seotud ülesannetes kaasa. Hädaolukorraametnik vastutab üleinstitutsioonilise hädaolukordade halduse koostamise, rakendamise, edasiarenduse ja nõustamise eest, samuti kõikide sinna juurde kuuluvate dokumentide ja reeglite eest. Hädaolukorraametnik koordineerib koostöös institutsiooni juhtkonnaga ressursside eraldamist sellistele töötajagruppidele, kelle ülesanneteks on hädaolukorraennetuse planeerimine ja hädaolukordade likvideerimine. Hädaolukorraametnik koordineerib hädaolukorraennetuse kontseptsiooni ja

hädaolukorrakäsiraamatu koostamist. Hädaolukorraametnik kontrollib meetmete ellurakendamist, planeerib hädaolukorraõppuste läbiviimist ja kooskõlastab oma planeerimistegevuse institutsiooni juhtkonnaga. Hädaolukorraametniku ülesandeks on pärast kahju tekitanud sündmuse esinemist hädaolukordade likvideerimise üldine alalüüs. Ta vastutab hädaolukorraõppuste tulemuste analüüsimise eest ja töötab koostöös organisatsiooni erinevate allüksustega välja meetmed, kuidas puuduseid kõrvaldada ning protsessi paremaks muuta. Hädaolukorraametnik nimetab ametisse vastutavad töötajad ja kontrollib nende tööd. Tema vastutuse alla kuulub hädaolukordade halduse kompetentse toimimise tagamine. Hädaolukorraametnik peab omal vastutusel heaks kiitma kõik hädaolukorrad käsitlevates dokumentides tehtavad muudatused.

Hädaolukorraametnikul on institutsiooni juhtkonna ees aruandluskohustus. Juhul, kui rakendatakse hädaolukorrakoordinaatoreid, on hädaolukorraametniku kohustuseks kutsuda kokku ja juhatada regulaarselt toimuvaid ühiseid koosolekuid. Hajali töötavate hädaolukorrakoordinaatorite tööd koordineerib hädaolukorraametnik. Hädaolukorraametnikul on õigus hädaolukorraennetuse planeerimise raames korraldusi jagada. Hädaolukorraametnik teeb ettekirjutusi protseduuride valiku kohta, annab ette tegutsemismustrid, liidab hädaolukorrakoordinaatorite töö üheks ja vormistab töötulemused institutsiooni jaoks ühtsustatud lõpptulemuseks.

Ei tohi unustada, et hädaolukorraametnikule on vaja ka kvalifitseeritud asendajat, kes peab olema alati hästi informeeritud sellest, milline on asjade kõige värskem seis.

Hädaolukorrakoordinaatorid
Suuremates institutsioonides võivad hädaolukorraametniku tööd toetada täiendavad hädaolukorrakoordinaatorid. Seda, kas ja kui palju hädaolukorrakoordinaatoreid ametisse nimetatakse, sõltub konkreetse institutsiooni liigist ja suurusest. Soovitatav on organisatsiooni iga loogilise allüksuse kohta ametisse nimetada üks hädaolukorrakoordinaator. Organisatsiooni allaüksusteks võivad olla erinevad asukohad või ka regioonid, samuti võivad need järgida organisatsiooni loogilist struktuuri.

Hädaolukorrakoordinaator on hädaolukorraametniku ja koordinaatori vastutusse antud organisatsiooni allüksuse vaheline lüli. Hädaolukorrakoordinaator töötab iseseisvalt ja teostab hädaolukordade haldusega seotud tegevusi talle määratud organisatsioonilises allüksuses. Ülesannete hulka kuuluvad nii tööprotsesside mõjuanalüüsi (BIA) tegemine, erialaselt korrektsete tööprotsessidega jätkamise plaanide koostamine kui ka oma organisatsioonilises allüksuses sobivate meetmete järjepidev kehtestamine ja ellurakendamine. Hädaolukorrakoordinaator aitab ette valmistada, läbi viia ja analüüsida oma valdkonna teste ja õppuseid. Ta analüüsib regulaarselt hädaolukorradokumentatsiooni toimimise ja ajakohasuse väljaselgitamiseks läbiviidavate kontrollide tulemusi (kontrollib hädaolukorraennetusplaane) ning töötab vajaduse korral oma valdkonna tarbeks välja täiendusi. Ühiskoosolekutel edastab hädaolukorrakoordinaator aruandlusinfo omal vastutusel hädaolukorraametnikule ja abistab hädaolukorraametnikku institutsiooni juhtkonnale mõeldud otsuste langetamise mallide väljatöötamises.

Hädaolukorraennetusmeeskond
Organisatsiooni allüksustest välja valitud eksperdid aitavad lahendada erialalisi küsimusi, tehes aeg-ajalt koostööd hädaolukorraennetusmeeskonnana. Eksperdid nõustavad hädaolukorrakoordinaatoreid või hädaolukorraametnikke spetsiifilistes teemades või viivad ellu hädaolukorraennetuse strateegilise planeerimise ettekirjutusi ja meetmeid. Vajadusel osalevad eksperdid ka testide ja hädaolukorraõppuste ettevalmistuses, korraldamises ja tulemuste analüüsimises.

4.3.2 Hädaolukordade likvideerimise töökorralduslik rollijaotus

Hädaolukordade ja kriiside likvideerimine eeldab eraldiseisvat töökorralduslikku struktuuri, mille põhjal kogutakse eriolukorra tarbeks kokku erinevad töötajad, arvestades eriolukorra liigi, ulatuslikkuse ja raskusastmega. Hädaolukordade likvideerimise töökorralduslikud rollid tuleb täpselt määratleda ja dokumenteerida ning need peavad kajastama ülesandeid, võimupädevust, vastutusi, teavitamiskohustusi, eskalatsioonietappe ja kindlasti ka õigusi. Töötajate jaotamine rollidesse peaks toimuma nende sobivuse põhjal, mitte hierarhilise positsiooni alusel, mida nad organisatsioonis täidavad, kuna ekstreemsed olukorrad seavad inimestele ka füüsilise ja psüühilise koormusega seotud spetsiaalsed nõuded. Mitte kõik funktsionäärid ei ole kohe automaatselt ka suure koormusega situatsioonides head strateegid ning võivad äärmuslikel juhtudel kriisistaabi tööd koguni pärssida. Juhtivtöötajad on harjunud, et neil on situatsiooni üle täielik kontroll, et nad saavad otsused lõpuni läbi mõelda ja erinevaid tagajärgi kaaluda. Kriisisituatsioonis kogetav „kontrolli kaotamine" või vajadus langetada otsuseid väga kiiresti, ilma et oleks teada, milline võib olla nende otsuste mõju töökohale ja karjäärile, võib tekitada inimestes tunde, et rünnatakse nende isikut. See aga võib viia täielikult halvatud tegutsemisvõimeni.

Juhtudel, kus töötajad võtavad enda kanda hädaolukordade likvideerimisega seotud töörolle, tuleks nende töölepingutes või vastavates lisalepingutes fikseerida kriisiolukordades kehtiv vastutuse välistamine või vastutuse piiramine.

Kuna hädaolukorra- ja kriisisituatsioonid eeldavad kiiret tegutsemist ning eriolukorras valitsevad tingimused võivad seda mitmeti takistada, tuleks iga töötaja kohta ametisse nimetada vähemalt üks või koguni mitu asendustöötajat.

Kriisiotsuste komitee

Hädaolukordade likvideerimise strateegiline vastutus lasub kriisiotsuste komiteel. Komitee moodustavad reeglina juhtkonna kõige kõrgema tasandi üks või mitu liiget, nt juhatuse liikmed, või ametiasutuse juhid. Kriisotsuste komitees istuvad „mõtlejad", kes annavad ette kriisi lahendamise strateegilise suuna ja langetavad laialdase mõjuga otsuseid, mis ületavad kriisistaabi juhile kehtestatud kompetentsi. Siia kuuluvad nt kriisisituatsiooni strateegilised otsused, mis ületavad hädaolukordade halduse kompetentsi või tööprotsessidega jätkamise strateegiad, millel võib olla institutsioonile pikaajaline mõju (nt mõne protsessi täielik seismapanek). Kriisiotsuste komitee üheks täiendavaks ülesandeks hädaolukorra likvideerimise raames on oluliste huvigruppidega kontakti loomine ja hoidmine.

Kriisiga seotud tööd tuleks sellele vaatamata siiski jätta kriisistaabi kanda. Kriisostuste komitee ja kriisistaabi koostöö tihedus sõltub institutsiooni liigist ja suurusest. Mõningates, eriti väikestes institutsioonides, on vastav eristamine ära jäetud ning kriisisotsuste komiteed esindab juhatuse kõige kõrgema astme üks liige, kes töötab kriisistaabi meeskonnas.

Kriisistaap

Kriisistaap on hädaolukorralikvideerimise keskne juhtimisorgan. Kriisistaabi mõiste on selle komisjoni puhul juurdunud sõltumata sellest, kas tegu on hädaolukorra või kriisi likvideerimisega. Seetõttu kasutatakse ka siin dokumendis läbivalt kriisistaabi mõistet.

Kriisistaap on planeeriv, koordineeriv, informeeriv, nõustav ja teostav üksus. Tegu on erilise, ajutise töökorraldusliku struktuuriga, mis lõhub vajadusel hädaolukorra kõrvaldamiseks organisatsiooni tavapärast struktuuri, ning seob endaga üleosakonnalised kompetentsid. Kriisistaabi töö aluseks on hierarhiavabade otsuste langetamine, mis tähendab, et kõik kriisistaabi liikmed on võrdsed. Kriisistaap planeerib, koordineerib, kohustab läbi viima ja kontrollib hädaolukorra likvideerimisega seotud tegevusi ning juhib kogu selleks vajaliku olulise teabe ja kõikide vajalike ressursside kättesaadavust.

Kriisistaap koosneb juhatajast, tuumikmeeskonnast ja täiendavast kriisistaabimeeskonnast. Vajadusel täiendatakse seda veel nõustavate spetsialistidega. Kriisistaabi täpne ülesehitus

sõltub ennekõike institutsiooni liigist, struktuurist ja suurusest. Kriisistaapi kokku kutsutavate töötajate valik sõltub kriisi liigist. Kehtima peaks põhimõte: võimalikult väike ja võimalikult hästi täiendatav.

Kõikides, ükskõik millist liiki organisatsiooni kriisistaapides tuleb tegeleda järgmiste ülesannetega.
- Olukorra fikseerimine ja hindamine. Kõiki olulisi andmeid tuleb regulaarselt värskendada.
- Hädaolukorra likvideerimisega seotud tööülesannete edastamine vastutavatele instantsidele ja selleks vajalike tegevuste koordineerimine.
- Koostöö ajakirjandusega ja sisekommunikatsiooni koordineerimine (kriiskommunikatsioon).
- Erinevate meetmete kooskõlastamine.

Igale kriisistaabi liikmele peab olema ette nähtud vähemalt üks asendaja, juhtivate funktsioonide puhul vähemalt kaks asendajat. Kriisistaabi juhi asendajate arvu puhul peetakse mõistlikuks kuni nelja asendajat. Läbivaks põhimõtteks on nõue, et kriisistaap peab olema ad hoc tegutsemisvõimeline.

Kriisistaabi juht ja tuumikmeeskond
Tuumikmeeskonna moodustavad kriisistaabi juht ja üks kuni viis oluliste funktsioonide kandjat. Nemad on meeskonna püsiliikmed. Kriisistaabi juht võtab vastu kõik hädaolukorra likvideerimisega seotud otsused. Hädaolukorra väljakuulutamisel kehtima hakkav kriisistaabi juhi laialdane võimupädevus, tegutsemise finantsraamistik ja õiguslik raamistik tuleb juba eelnevalt kindlaks määrata.

Situatsioonis, kus hädaolukord on juba välja kuulutatud, otsustab kriisistaabi juht konkreetse sündmuse põhjal kokkukutsutava kriisistaabi suuruse ja liikmete üle. Kriisistaabi juht määrab, kus kohas ja millises ruumis hakatakse kriisistaabi tööd tegema ning fikseerib, millised organisatsioonivaldkonnad on kriisist puudutatud, sest kriisistaabi õigus jagada korraldusi kehtib ainult kriisvaldkondadele. Organisatsiooni allüksustes, mida kriis ei puuduta, jäävad endiselt kehtima tavapärased kompetentsid. Nende juhtumite puhuks, kus juhti ei õnnestu kätte saada, tuleb vastu võtta otsus selle kohta, kes teda asendab. Reeglina valitakse asendajaks keegi kriisistaabi töötajate hulgast.

Tagamaks hädaolukorras kogenud ja koordineeritud töömeetodite toimimist, peaks tuumikmeeskond koosnema samadest isikutest võimalikult pikema aja jooksul. Praktilised kogemused on näidanud, et tuumikmeeskond peaks täitma järgmisi funktsioone:

- töö avalikkusega, seistes hea asutuse või ettevõtte kommunikatsiooni eest, ning
- ametiasutuse või ettevõtte turvalisuse tagamine nii infoturbe kui ka tööohutuse seisukohalt (ingl Safety and Security).
Sõltuvalt institutsiooni eripäradest võib tuumikmeeskonna liikmete hulka kuuluda ka IT-käitusvaldkonna esindaja.

Kuna kriisistaabi töötajad peavad suutma ekstreemsetes oludes kaalutletult ja sihikindlalt tegutseda ning sealjuures ka tundlike aspektide ja pidevalt muutuvate faktorite omavahelisi mõjutusi läbi kaaluda, tuleb selle liikmete valikul olla väga hoolikas. Liikmeid tuleb ka vastavalt koolitada. Kriisistaabi juhilt eeldatakse, et tal peaks olema tugev juhiisiksus, kõrge koormustaluvus ekstreemsituatsioonides, samuti kõrge stressitaluvus ning võime langetada otsuseid ka ajalise survega situatsioonides. Valmidus meeskonnatööks ja sotsiaalne pädevus on samuti omadused, mida kriisistaabi juhilt võiks oodata.

Kriisistaabi täiendatud meeskond
Täiendatud kriisistaap koosneb eriülesannete täitjatest või abigruppidest, keda on sõltuvalt hädaolukorra liigist võimalik täiendavate abijõududena kriisistaabi töösse lülitada. Seetõttu räägitakse siinkohal staabi sündmustepõhistest liikmetest. Nende hulka kuuluvad näiteks:

- IT-administraatorid / IT-juht (juhul, kui nad ei kuulu tuumikmeeskonda),
- asukoha turvalisuse eest vastutavad töötajad, nt tuleohutusspetsialist, keskkonnakaitse spetsialist, seadmete turvalisuse spetsialist, päästeteenistus,
- CERT-i juht, juhul, kui CERT (Computer Emergency Response Team) on olemas,
- õigusnõunik,
- personalijuht,
- kontaktisikud puudutatud osakondadest ja töövaldkondadest, nt müük, logistika jne,
- kontaktisikud, kelle vastutusalaks on varumisosakond, finantsosakond, tehnikaosakond, sisekommunikatsiooni osakond, personaliosakond,
- andmekaitsespetsialist ja
- konfidentsiaalsusspetsialist.

Erilisel kohal kriisistaabi töötajate hulgas on hädaolukorraametnik, kes toetab kriisstaabi tööd ja nõustab kriisistaapi ennekõike hädaolukordadega seotud planeerimise vallas. Lisaks erialaspetsialistidele peaks kriisistaabi liikmete hulgas leiduma ka sekretäre (kriisistaabi assistente), kes toetavad staabi administratiivseid tegevusi, samuti protokollija, kes tagab kõikide sündmuste ja langetatud otsuste revisjonikindla protokollimise.

Kriisistaabi erialanõustajad
Ühelt poolt tuleks hoolitseda selle eest, et kriisistaapi liikmetega üle ei koormataks (maksimaalselt 10 liiget), teiselt poolt jällegi tuleb tagada, et iga hädaolukorra puhul saaksid vajalikud ülesanded ja funktsioonid kaetud. Üheks võimaluseks, kuidas kriisistaapi mitte lõhki ajada, on kaasata väliseid eksperte, keda kriisistaabi liikmete hulka ei liigitata. See kehtib eriti selliste kriiside puhul, mida institutsiooni oma jõududega ei suudeta ületada, nt kriminaalse taustaga kriisid nagu väljapressimine, inimröov või pommiähvardus.

Hädaolukorrameeskonnad
Hädaolukorralikvideerimise operatiivse poole lahendavad erinevad hädaolukorrameeskonnad. Nende ülesandeks on tööprotseduuride, rakenduste või süsteemide taaskäivitamine ja taastamine. Klassikaliste hädaolukorrameeskondadena on tuntud infrastruktuur, IT ja erialavaldkonnad. Hädaolukorrameeskonnad peavad hädaolukordade likvideerimise raames eranditult kriisistaabi korraldusi järgima.

Infrastruktuuri hädaolukorrameeskond vastutab hoone kasutamisvõimaluse ja hoones asuvate töökohtade kasutamisvõimaluse taastamise eest. Siia alla kuuluvad elektrivarustuse ja kliimaseadmete töö taastamine, võrkude ümberlülitamine, asendustöökohtade sisseseadmine, töövahenditega varustamine ja töövahendite utiliseerimine, samuti kaablite ümberpaigaldamine.

IT-hädaolukorrameeskonna ülesannete hulka kuulub muuhulgas varusüsteemide hankimine, nende töölerakendamine, andmete taastamine ning telefonikeskjaama võimalike rikete likvideerimine.

Organisatsiooni allüksuste (nt ettevõtlus) eest vastutavad hädaolukorrameeskonnad vastutavad kohapealsete meetmete rakendamise eest, mis tagavad tootmis- või tööprotsesside taaskäivitamise. Siia alla kuuluvad tööprotsesside alustamine asendustöökohtades, asendusprotseduuride rakendamine või tööprotsesside tagamine vähendatud võimsusel ning lõpuks tavapäraste tööprotsesside taastamine. Kõik see toimub koostöös erialavaldkondade hädaolukorrameeskondadega. Erialavaldkondade hädaolukorrameeskondade juhid (erialavaldkondade koordinaatorid) vastutavad oma valdkonnas tööprotsesside jätkamise plaanide ellurakendamise eest.

Hädaolukorrameeskondade juhid on kohustatud hädaolukordade likvideerimise raames kriisistaabile regulaarselt aru andma. Meeskondade juhid koguvad kohapeal andmeid, saadavad andmed edasi kriisistaapi ja koordineerivad ning kontrollivad kohapeal kriisistaabi kehtestatud meetmete rakendamist. Vajadusel algatavad juhid kahju tekkimise asukohas

asendusmeetmed ja loovad kontaktivõimaluse väliste abijõudude nagu politsei, päästeteenistuse või tuletõrje kaasamiseks. Ajakirjanduse küsimused tuleks sellele vaatamata siiski edasi suunata kriisistaapi või kriisikommunikatsioonikeskusesse.

Täiendav abipersonal
Sõltuvalt institutsiooni liigist ja võimalikust kahjustsenaariumist võib olla vajalik töötajate, nende lähedaste või muude puudutatud isikute tarbeks protsessi kaasata ka psühholoogilised nõustajad. Suurte kahjudega sündmused toovad endaga sageli kaasa suure psüühilise koormuse, eriti neil juhtudel, kus leidub kannatanuid. Juhul, kui institutsioonil on olemas oma palgalised psühholoogid, oleks mõistlik neid koolitada, et nad oskaksid inimesi katastroofis nõustada, aga ka abistada ja nõustada kriisistaabi tööd.

Mitu asukohta
Olukorras, kus institutsioon töötab mitmes asukohas, mis asuvad hajali võib-olla terves maailmas, saab hädaolukordade likvideerimise töökorralduses valida mitmete erinevate mudelite vahel.
- Ehitada igas asukohas kogu struktuur eraldi üles, alates kriisiotsuste komiteest ja lõpetades hädaolukorrameeskondadega. Asukohtadeülene koordineerimine tuleks anda täiendava (vajadusel rahvusvahelise) otsustuskomisjoni kanda.
- Igas asukohas on lokaalne kriisistaap ja lokaalsed hädaolukorrameeskonnad. Asukohtadeülest tegevust koordineeritakse keskse kriisotsustuskomisjoni kaudu.
- Mõlemad, nii otsustuskomisjon kui ka kriisistaap, töötavad tsentraliseeritult, kohapeal töötavad ainult operatiivsed hädaolukorrameeskonnad.

Asukoha piiridest väljuva kriisi likvideerimiseks sobiva mudeli valimine sõltub ennekõike institutsiooni üldisest struktuurist, erinevate asukohtade suurusest, asukohtade omavahelistest sõltuvussuhetest ja nende geograafilisest paiknemisest üksteise suhtes. Otsus tuleb teha iga juhtumi puhul eraldi.

4.3.3 Koostöö infoturbehaldusega

Lisaks hädaolukorraennetuse ja hädaolukordade likvideerimise valdkonnale peaksid igas institutsioonis olemas olema ka töökohad ja vastutusalad, mis kataksid infoturbehalduse valdkonna. Seepärast peaks igas institutsioonis lisaks hädaolukorraametnikule olema ka IT-turvaspetsialist, kes vastutaks kogu institutsiooni infoturbe valdkonna eest.

Kuna siin on mõningaid kattuvusi hädaolukordade halduse ja infoturbe halduse kontseptsiooniga, tuleks selgitada, kui suures osas suudaks hädaolukorraametnik üle võtta IT-turvaspetsialisti tööülesanded, või mil määral suudaks IT-turvaspetsialist täita mõnd hädaolukordade halduses ettenähtud rolli. Vastavad rollid ei välista teineteist lõplikult. Määravaks on institutsiooni liik ja tegevusvaldkond, tööprotsesside sõltuvus IT-st ja turvahalduse süsteem. Mida rohkem tööprotsessid IT toimimisest sõltuvad, seda suurem on ka erinevate valdkondade kattuvus. Turvahaldus peab käsitlema institutsiooni tervikuna ja protsessidest lähtuvalt, mitte IT-põhiselt. Kui see tingimus on täidetud, on mõistlik, et IT-turvaspetsialisti ja hädaolukorraametniku funktsiooni täidab üks isik.

Sellele vaatamata tuleks juba varem selgusele jõuda järgmistes olulistes aspektides.

- Erinevate tööülesannete kokkupuutepunktid peavad olema selgelt defineeritud ja dokumenteeritud. Lisaks peaksid mõlema töökoha puhul olemas olema selged aruandluskohustused, mis on suunatud töötajast ülespoole. Ideaaljuhul võiksid aruandluskohustused olla identse suunitlusega ning ka adressaadiks võiks olla juhatuse kõige kõrgema astme üks ja sama isik.
- Tuleks kaaluda, kas konfliktsete teemade puhul tuleks teavitada institutsioonisisest revisjoni.
- Tuleb tagada, et erinevaid tööülesandeid samaaegselt täitvad töötajad oleksid piisavalt kvalifitseeritud ja et neil oleks oma ülesannete täitmiseks piisavalt ressursse.

4.4 Hädaolukordade halduse poliitika koostamine

Hädaolukordade halduse olulisus organisatsioonis ja selle strateegiline suund tuleb kokku võtta hädaolukordade halduse poliitikas. See on hädaolukordade halduse kontseptsiooni, ülesehituse ja tööshoidmise raamiks. Poliitikaga kirjeldatakse piiratud lehekülgedel seda, milleks on hädaolukordade haldust vaja ja millised on selle eesmärgid.

Poliitika koostamise võtab enda peale vastavaid kvalifikatsioone omav meeskond. Hädaolukorraametniku ülesandeks on seejuures koordineerimine. Kuna hädaolukordade halduse poliitika on keskse tähtsusega strateegiline dokument, peaks see olema sellise ülesehitusega, et selle sisu oleks organisatsiooni kõikidele asjassepuutuvatele osakondadele arusaadav. Seetõttu on üldise vastuvõtlikkuse tagamiseks mõistlik organisatsiooni juhtkonna kõrval kaasata koostamisse ka võimalikult palju allosakondi. Lisaks osakondadele on soovitatav kaasata töötajate esindaja, ettevõtte/ametiasutuse ohutuse esindaja (info- ja tööohutus), siserevident, riskihaldus, ettevõtte/ametiasutuse sideosakond, infotehnoloog või ka juristid. Siiski võib ja peab iga organisatsioon nende vajaduse üle ise otsustama.

Hädaolukordade halduse poliitika sisu

Hädaolukordade halduse poliitika peab olema lühike ja ülevaatlik ning sisaldama vähemalt järgnevaid aspekte:
- hädaolukordade halduse definitsioon,
- hädaolukordade halduse olulisus organisatsiooni jaoks,
- eesmärk,
- hädaolukorrastrateegia tuum,
- kehtivusala,
- aluseks olev hädaolukordade halduse tegutsemismudel või aluseks olev standard (nt BSI standard 100-4),
- ülesehituse struktuur koos olulisemate rollide ja nende vastutusaladega,
- institutsiooni juhtkonna kohustus hädaolukordade haldust optimeerida, kasutades regulaarseid kontrolle, teste ja õppuseid,
- asjassepuutuvad seadused, direktiivid ja eeskirjad, millega tuleb arvestada ja
- vastutuse võtmine institutsiooni juhatuse poolt, mis dokumenteeritakse täiendavalt selge, kinnitava allkirjaga.

Vajadusel võib nimetada ka üldiseid hädaolukordade halduse järelevalve ja tulemuslikkuse kontrolli kohta käivaid tingimusi.

Poliitika avalikustamine

Hädaolukordade halduse poliitika peab olema organisatsioonisiseselt avaldatud ja edastatud kõikidele töötajatele ja potentsiaalsetele huvigruppidele. Hädaolukordade halduse protsessides osalejatele tuleb poliitikast eraldi teada anda ja nad peavad oma teadlikkust allkirjaga kinnitama.

Poliitika uuendamine

Poliitikat tuleb uuendada regulaarselt, vajadusel ka siis, kui muutuvad raamtingimused, ärieesmärgid, ülesanded või strateegia. Koordineeriv vastutus selle täideviimise eest lasub hädaolukorraametnikul. Uuendamine tuleb kooskõlastada juhtkonnaga. Juhtkond peab uuenenud poliitika allkirjaga kinnitama ja selle edastama.

4.5 Ressursside eraldamine

Hädaolukordade halduse loomine ja tööshoidmine eeldab finantsressursse, personali ja aega. Selle asjaoluga tuleb hädaolukorrastrateegia kindlaksmääramisel ja kriitiliste äriprotsesside kaitsmise poole püüdlemisel arvestada. Eesmärgiks seatud kaitsetase peab olema majanduslikult mõistlik. Hädaolukordade halduse jaoks vajaminevate ressursside hulk sõltub olulisel määral organisatsiooni suurusest ja tüübist, ettevõtte liigist ja asukohast, keskkonnast, klientidest, kasutatavast tehnoloogiast ning ka organisatsiooni riskivalmidusest.

4.5.1 Kuluefektiivne hädaolukorrastrateegia

Kuluefektiivse hädaolukorrastrateegia koostamiseks tuleb investeeringuid võrrelda nendest saadava kasu ja tegeliku kaitsevajadusega. Tuludeks saab lugeda hädaolukorraolukorraga või kriitiliste äriprotsesside tõrkega kaasnevate kulude vältimist. Nõnda on hädaolukordade haldusel infoturbe haldussüsteemiga samad, põhjendamisel ja juhatuse veenmisel tekkivad probleemid.

Välditud kulud koosnevad otsestest ja kaudsetest kuludest. Otseste kulude hulka kuuluvad nt väiksem käive või tellimuste kaotamine, katkestused tootmises, lepingute või seaduste mittejärgimisest tulenevad karistused ja süsteemide taastamise kulud. Kaudsed kulud võivad olla väga erinevad. Nende alla kuuluvad näiteks imidži kahjustumine ja usaldusväärsuse kaotamine. Nende tagajärjeks võib omakorda olla klientide kadu või turupositsiooni nõrgenemine, samuti suuremad investeeringud uute klientide leidmiseks või vanade usalduse tagasivõitmiseks.

Kuna projekti alguses on hädaolukordade halduse juurutamiseks vajalikud kulude ja tulude hinnangud väga umbkaudsed, tuleks esialgset hädaolukorrastrateegiat projekti käigus ning hädaolukordade halduse kasutamisel regulaarselt kontrollida. Töökatkestuste ja investeeringute täpsemad andmed saadakse alles mõne aja möödudes. Kui soovid ja tegelikud finantsvõimalused on liiga erinevad, tuleks hädaolukorrastrateegiat kohandada.

4.5.2 Hädaolukordade halduse töökorralduseks vajalikud ressursid

Hädaolukordade halduse tööshoidmine ja ülesehitamine eeldavad personaliressursside olemasolu. Hädaolukordade halduse juurutamisel tuleks hädaolukorraametnik ja vajadusel ka hädaolukorrakoordinaatorid oma muudest ülesannetest vabastada, et võimaldada halduse kiiremat rakendamist. Sõltuvalt organisatsiooni suurusest võivad need töötajad täita hädaolukordade haldusega seotud ülesandeid oma tavapäraste tööülesannete kõrvalt. Ainult vähesed organisatsioonid suudavad hädaolukorrakoordinaatoritele või hädaolukorraennetamise meeskonnale täistöökohti luua.

Ressursse ei vajata mitte ainult hädaolukordade ennetamisel. Hädaolukorra kõrvaldamiseks vajaminevate töötajate ajakulu ei tohi alahinnata. Isegi kui neid ei lähe tarvis kriisi aktiivseks lahendamiseks, peavad nad siiski osalema vajalike testide ja õppuste läbiviimises. Sõltuvalt organisatsiooni jaoks vajaminevatest õppustest tuleb töötajad järk-järgult oma tavaülesannetest vabastada.

Samuti tuleb tagada piisavate ressursside olemasolu, et oleks võimalik hädaolukorrameetmete ning hädaolukordade haldusprotsessi tõhusust ja sobivust süstemaatiliselt ja regulaarselt kontrollida. Kontrollide käigus tuleks vaadelda ka kasutatavaid ressursse ja nende efektiivsust. Kui selgub, et teatud meetmed põhjustavad ebamajanduslikult kõrgeid kulusid, tuleks otsida alternatiivseid meetmeid ning kaaluda, kas muuta võib-olla järjepidevusstrateegiat (vt ptk 5.4), BIA nõudeid või lausa hädaolukorrastrateegiat. Samuti tuleb personaliressursside planeerimisel arvestada parandusettepanekute juurutamise ja rakendamisega ning tuvastatud puuduste kõrvaldamisega.

Reaalses olukorras puudub organisatsiooni hädaolukordade halduse eest vastutaval töötajal sageli aeg, et analüüsida kõiki olulisi mõjufaktoreid ja raamtingimusi (nt seaduseid või tehnilisi küsimusi). Mõnikord pole töötajatel projekti alguses ka veel vajalikke algteadmisi. Sellisel juhul võib olla mõistlik kasutada organisatsioonivälise ekspertide abi. Hädaolukorraametnik peab vastava info edastama ja dokumenteerima, et juhtkond saaks selleks piisavalt ressursse eraldada.

4.5.3 Ennetavate meetmete ressursid ja nende rakendamine

Ennetavate meetmete hulka kuuluvad isiklike meetmete kõrval ka organisatoorsed meetmed, infrastruktuuri meetmed ja tehnilised meetmed. Sobivate meetmete valimisel tuleks püüelda nende kõigi mõistliku kasutamise poole korraga. Sageli on investeeringud personaliressurssidesse ja organisatoorsed reeglid tõhusamad kui tehnoloogiasse tehtavad investeeringud. Tehnoloogia ei suuda üksinda probleeme lahendada. Tehnilised ja infrastruktuurilised meetmed tuleb alati siduda sobiva töökorraldusliku raamistikuga. Sellegipoolest on oluline, et tehnilisi meetmeid kasutataks õigesti. Määravaks on nii valik, administreerimine kui ka töökindluse regulaarne testimine. Investeeringud tehnoloogiasse, mis hädaolukorraolukorraga toime ei tule, on mõttetud.

4.5.4 Koostöö teiste haldussüsteemidega

Nagu edasistest peatükkidest on võimalik välja lugeda, kattub hädaolukordade haldus osaliselt teiste haldussüsteemidega, nt infoturbe haldussüsteemi ja (IT-)riskihaldusega. Haldussüsteemide edu ja kulude peamisteks faktoriteks on hädaolukordade halduse mõistlik sidumine olemasolevate struktuuridega, hea kommunikatsioon ettevõtte või ametiasutuse erinevate osakondade ning ärivaldkondade vahel, vajaliku info avatud ja konstruktiivne edastamine ning selge ülesannete jaotamine. Haldussüsteemide valdkondade sihipärase ja aegsa koostöö abil saab ära kasutada sünergiaefekte ja säästa raha, personali ning aega.

4.6 Kõikide töötajate kaasamine

Hädaolukordade halduse edukaks juurutamiseks ja tööshoidmiseks tuleks see sarnaselt teistele kõikehõlmavatele haldussüsteemidele kindlalt siduda ametiasutuse/ettevõtte tööprotsessidega. Hädaolukordade haldus puudutab, olgugi et erineval määral, eranditult kõiki töötajaid. Igaüks võib vastustundliku ja riskiteadliku tegutsemisega anda oma panuse kahjude vältimisse ja hädaolukordade halduse edukasse toimimisse. Töötajate teadlikkuse tõstmine ja koolitamine on selle hädavajalik eeldus. Esimeseks sammuks on hädaolukordade halduse poliitika avaldamine. Ka töökliima, ühised väärtused ja töötajate soov endast parimat anda on äriprotsesside ja seega ka organisatsiooni tugevuse tagamisel olulised.

4.6.1 Töötajate teadlikkuse tõstmine ja koolitamine

Hädaolukordade halduse elutsüklis olulisel kohal on tõsta töötajate teadlikkust hädaolukordade halduse teemade kohta. Teavitamis- ja koolitamisprogramm, aga ka temaatilised üritused peavad tagama, et kõik organisatsiooni töötajad teavad, et hädaolukordade haldus on olemas, teavad, mis on selle halduse eesmärk, kuidas eduka hädaolukordade halduse elluviimisesse ja käigushoidmisesse panustada ja kuidas käituda hädaolukorra korral. Kuna kõik töötajad ei vaja samal määral teavitamist, tuleks tegutseda lähtuvalt sihtgruppidest ja vajadusest. Teadlikkuse tõstmise ning koolituse põhjalikkus ja liik tuleb valida vastavalt vajadusele.

Koolitused peavad nii hädaolukorraennetuse kui ka hädaolukorra likvideerimise töötajaid oma ülesanneteks sihikindlalt ette valmistama ja andma neile vajaliku kvalifikatsiooni. Koolituskontseptsiooni koostamiseks tuleb esmalt tuvastada koolitusvajadus ja see dokumenteerida. Järgmise sammuna tuleb tuvastada teemad ja sisu (näiteks tööprotsesside mõjuanalüüs, riskianalüüs, ajakirjandusega suhtlemine, hädaolukorrakõrvaldamismeeskonna liikmete treenimine).

Koolituseks/treeninguks saab kasutada nt alljärgnevaid meetodeid:
- arvuti- või internetipõhine õpe,
- üksik- või grupitreening või organisatsioonisisesed või
-välised seminarid,
mis tuleb välja valida ja dokumenteerida.

Teadlikkuse tõstmiseks tuleks kasutada ametiasutuses/ettevõttes juba olemasolevaid sidemeetodeid, nt juhtivtöötajate koosolekuid, regulaarsed koosolekuid, uusi töötajaid juhendavaid üritusi, organisatsiooni allüksuste üritusi, töötajate ajakirju, plakateid või uudiskirju. Mõistlik oleks kooskõlastada meetmed turva- või riskihalduse teavitamisprotseduuridega ja teha nendega koostööd.

Organisatsiooni allüksuste juhid peaksid oma töötajate koolitust ja aktiivset osalemist toetama ja töötajad nende meetmete jaoks igapäevastest tööülesannetest vabastama. Pärast teavitamis- ja koolitamismeetodite läbiviimist tuleks kontrollida, kas töötajatele on need meelde jäänud ja kas nad on nendest õigesti aru saanud. Koolitus- ja teavituskava elluviimine ja edusammud tuleb dokumenteerida. Läbiviividud koolituste tõendid tuleb alles hoida. Soovitatav oleks läbiviidud teavitus- ja koolitusmeetmete tõhusust hinnata. Organisatsiooni juhtkonda tuleb kord aastas meetmete olukorrast teavitada.

4.6.2 Töötajate kaasamine, riskikommunikatsioon ja varajane tuvastamine

Organisatsiooni vastupanuvõime suurendamiseks ja hädaolukorraks ettevalmistamiseks tuleb lisaks töötajate regulaarsele teavitamisele luua ka sobivad struktuurid, et hädaolukordade halduse aktiivne rakendamine oleks võimalik. Selleks tuleb määrata kontaktisikud ja vastutusalad ning need kõigile teatavaks teha.

Töötajad tuleb kaasata regulaarsesse riskide, intsidentide ja mõjude infovoogu. Kui töötajad tuvastavad argitöös ettevõtlust ohustavaid riske või isegi kui on olemas ainult vastav kahtlus, peaks iga töötaja teadma, kuidas käituda ja keda olukorrast teavitada. Sellist aktiivset võimalikest riskidest teavitamist nimetatakse hädaolukordade halduse vallas ka riskikommunikatsiooniks. See võib aidata riske varakult tuvastada ja vastumeetmeid tarvitusele võtta, et hädaolukorrad ära hoida või selle tagajärgedega kiiremini toime tulla.

5 Kontseptsioon

Hädaolukorraennetuse kontseptsioonist (vt ptk 5.5) ja hädaolukorrakäsiraamatust (vt ptk 7.4) koosneva hädaolukorrakontseptsiooni väljatöötamine eeldab mitmeid ettevalmistusi. Selle eesmärgiks on mõista ettevõtet/ametiasutust ja selle „tegevust", tuvastada käideldavusnõudeid, leida kitsaskohti, juurutada vastumeetmeid ja olla töökõlbulike hädaolukorraolukorra likvideerimismeetmetega valmis jääkriskidega toimetulemiseks.

Kriitiliste tööprotsesside ja ressursside kohta annab vajalikku infot Business Impact Analysis (tööprotsesside mõjuanalüüs, BIA). Vajalikku infot olemasolevate riskide kohta, mille eest organisatsioon end kaitsma peaks, pakub riskianalüüs. Järjepidevusstrateegia valikute väljatöötamine pakub võimalikke alternatiivne, kuidas meetmeid ellu viia. Juhatuse otsusega valitakse sobivad järjepidevusstrateegiad, mis moodustavad kontseptsiooni ja plaani koostamise raamistiku.

5.1 Tööprotsesside mõjuanalüüs (Business Impact Analysis)

Tööprotsesside mõjuanalüüsi peaülesandeks on mõista, millised tööprotsessid on ettevõtluse ja seega ka organisatsiooni säilimiseks olulised ja millised oleksid nende katkemise tagajärjed. Neid „kriitilisi" tööprotsesse kaitstakse hädaolukordade halduse raames eriti hoolikalt ja nende suhtes valmistutakse ette kriisiolukorraks.

Hädaolukordade halduse kontekstis tähendab „kriitiline” ajalises mõttes kriitilist, mis tähendab, et vastav protsess eeldab tegevuse kiiret jätkamist, kuna vastasel korral on kahjud organisatsiooni jaoks väga suured. Suureks kahjuks võib olla rahaline kahju, seaduste või lepingute rikkumine, imidži kahjustumine või muud kahjud. BIA käigus „mittekriitiliseks” liigitatud tööprotsess ei tähenda seda, et see pole organisatsiooni jaoks oluline, vaid seda, et selle taastamine on madalama prioriteediga.

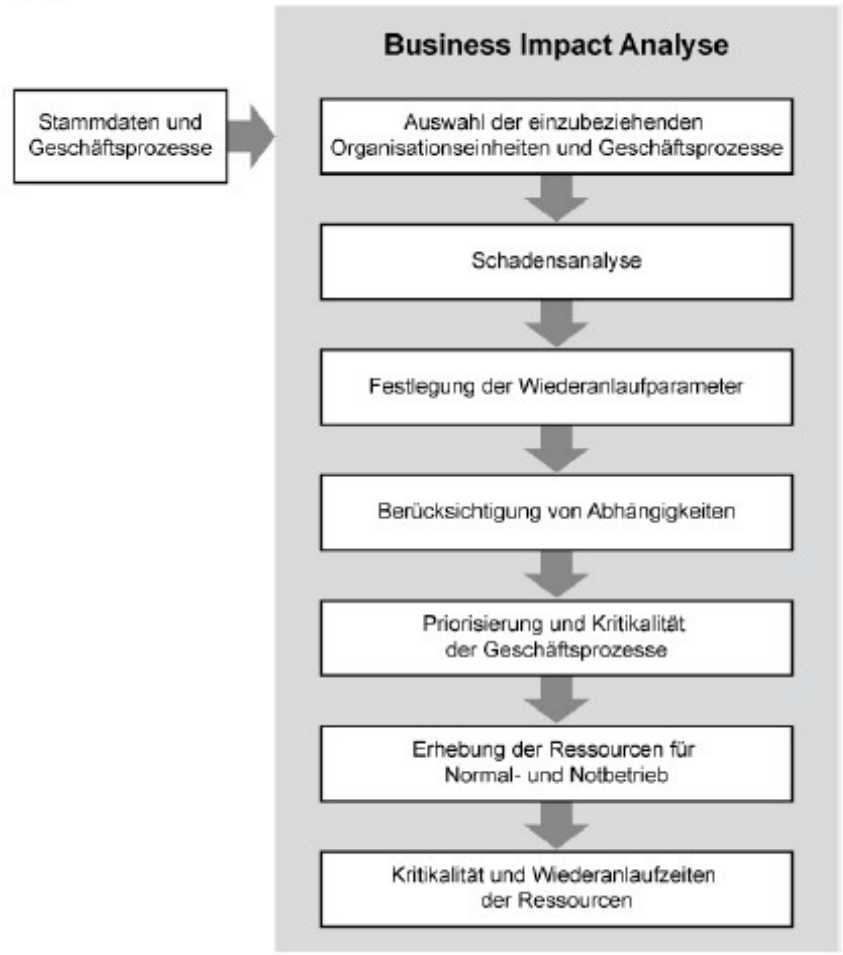
Selleks, et „kriitilisi” äriprotsesse tuvastada ja sobivaid strateegiaid ning kahjujuhtumite ennetamiseks sobivaid meetmeid välja töötada, tuleb esmalt tuvastada, millist mõju avaldaksid organisatsioonile tõrked, katkestused või lausa tööprotsesside täielik peatumine. Selleks tuleb tuvastada organisatsiooni olulisemad tooted ja teenused ning nendega seotud protsessid. Kriitilised tööprotsessid on reeglina kas tähtsate teenuste pakkumise või toodete tootmise jaoks väga olulised, kuid sellele vaatamata ei tohiks keskenduda üksnes nendele protsessidele.

Selles hädaolukordade halduse faasis pole hädaolukorra põhjus veel oluline, loevad ainult võimalikud tagajärjed, millega organisatsioon peab arvestama. Selleks kasutatakse tööprotsesside mõjuanalüüsi (Business Impact Analysis, BIA), mida saksa keeles tuntakse ka kui järelmõjude hindamist või tööprotsesside katkemise analüüsi. Tööprotsesside mõjuanalüüs aitab leida tööprotsesside taaskäivitamispunkte, leida taaskäivitamise prioriteete ja tuvastada sellega tööprotsesside kriitilisust ning vajaminevaid ressursse.

Tööprotsesside mõjuanalüüsi tegemiseks on mitmeid võimalusi. Ei ole olemas üht ja ainukest „õiget” meetodit, mida tuleks kindlasti eelistada. Vajalike tulemusteni jõudmise meetodi võib iga organisatsioon enda jaoks ise leida. Selles standardis tutvustatakse meetodit, mis toetub turbeastme tuvastamisele vastavalt BSI standardile 100-2, mis käsitleb infoturbe haldussüsteemi ülesehitamist vastavalt IT-etalonturbe nõuetele. BIA ja BSI standardile 100-2 vastava turbeastme väljaselgitamine on oma meetoditelt teatud määral sarnased, mistõttu saab ära kasutada nende sünergiat. Mõlema valdkonna koostöö või vähemalt põhjaliku infovahetusega saab vähendada mõlema töömahtu. Järgnevalt selgitatakse, millised on nende ühised jooned ja kuidas turbeastme määramist täiustada, et saada tulemuseks tööprotsesside mõjuanalüüs (BIA).

5.1.1 Ülevaade

Tööprotsesside mõjuanalüüsi saab jaotada järgnevateks sammudeks (vt joonis 3):
Tööprotsesside mõjuanalüüs (BIA)



Joonis 3. Tööprotsesside mõjuanalüüsi ülevaade

Stammdaten und Geschäftsprozesse – algandmed ja äriprotsessid;
Auswahl der einzubeziehenden Organisationseinheiten und Geschäftsprozesse – protsessi kaasatavate organisatsiooni allüksuste ja tööprotsesside valimine;
Schadensanalyse – kahjude analüüs;
Festlegung der Wideranlaufparameter – taaskäivitamisparameetrite määratlemine;
Berücksichtigung von Abhängigkeiten – sõltuvussuhetega arvestamine;
Priorisierung und Kritikalität der Geschäftsprozesse – tööprotsesside prioriteetide ja kriitilisuse määratlemine;
Erhebung der Ressourcen für Normal- und Notbetrieb – tavakäituseks ja hädaolukorrakäituseks vajalike ressursside väljaselgitamine;
Kritikalität und Wiederanlaufzeiten der Ressourcen – ressursside kriitilisus ja taaskäivitusajad

0. samm: algandmed ja äriprotsessid

Tööprotsesside mõjuanalüüsi tegemiseks läheb tarvis ülevaadet ettevõtte kõikidest olulistest äriprotsessidest koos vastutavate kontaktisikutega või ametiasutuse kõikidest tööülesannetest koos protsesside eest vastutavate isikutega. See ülevaade peaks lisaks protsesside loetelule sisaldama ka protsesside seost ärieesmärkidega ja näitama, milline on erinevate protsesside omavaheline sõltuvuslik seos. Ametiasutuse tegevuse eesmärgid on tavaliselt seadusega määratud. Kui protsessidest pole värsket ülevaadet, tuleb see kas tööprotsesside mõjuanalüüsi eeltööna koostada või olemasolevat värskendada. Lisaks tuleb koostada ülevaade organisatsiooni algandmetest nagu ettevõtte struktuur ja asukohad.

1. samm: protsessi kaasatavate organisatsiooni allüksuste ja tööprotsesside valimine
Kui on ilmselge, et hädaolukordade halduse kehtivusala piires on organisatsiooni mõningate allüksuste või tööprotsesside osakaal ärieesmärkide ja väärtuseid loovate tegevuste saavutamisel väga väike, siis võib need edasisest analüüsist välja jätta.

2. samm: Kahjude analüüs
Kahjude analüüsis vaadeldakse, millised võivad olla organisatsiooni kahjud juhul, kui erinevad tööprotsessid peaksid katkema. Siinkohal ei ole oluline mitte ainult kahju suurus, vaid ka selle ajaline kestus. Kahjude analüüsi tegemiseks tuleb kindlaks määrata uuritavad raamtingimused (kahjude kategooriad ja stsenaariumid), hindamisperioodid ning spetsiaalsete tähtaegadega toimetuleku strateegia, mille puhul on mõne protsessi käideldavuse nõuded keskmisest erinevad. Seejärel tuvastatakse iga üksiku protsessi ja iga hindamisperioodi puhul katkestuse tõttu tekkiv kahju.

3. samm: taaskäivitamisparameetrite määratlemine
Tuginedes kahju kestusele ja oodatava kahju suurusele, määratakse igale tööprotsessile maksimaalselt vastuvõetav katkestusaeg, taaskäivitamisaeg ja taaskäivitamise nivoo. Tulemustest tehakse lõpuks kokkuvõte ja andmed konsolideeritakse.

4. samm: sõltuvussuhetega arvestamine
Kuna taaskäivitamise parameetrid määrati kindlaks üksikute protsesside alusel, tuleks need kooskõlastada. Seejuures võetakse arvesse protsesside omavahelisi seoseid ja strateegilisi ärieesmärke ning vajadusel muudetakse parameetreid.

5. samm: tööprotsesside prioriteetide ja kriitilisuse määratlemine
Taaskäivitamise ja kahjude andmete alusel määratakse kindlaks tööprotsesside taaskäivitamise järjekord ja kriitilisus. Selleks tuleb määratleda kriitilisuse kategooriad ja nende piirid.

6. samm: tavakäituseks ja hädaolukorrakäituseks vajalike ressursside väljaselgitamine
Järjepidevusstrateegiate väljatöötamiseks ja ennetavate meetmete määratlemiseks tuleb tuvastada kriitilistes äriprotsessides kasutatavad ressursid. Välja tuleb selgitada nii tavarežiimi kui ka hädaolukorrarežiimi jaoks vajalike ressursside liik ja mahud. Inforessursi jaoks määratakse täiendavalt kindlaks ka maksimaalne lubatud andmekadu, millega tuleb pärast niinimetatud taastepunkti kasutamist arvestada.

7. samm: ressursside kriitilisus ja taaskäivitusajad
Tööprotsesside mõjuanalüüsi viimase sammuna tuvastatakse kriitilistes protsessides kasutatavad ressursid, taaskäivitamis- ja taastamisajad ning nende kriitilisus.

5.1.2 Tööprotsesside mõjuanalüüsi (BIA) teostus

Järgnevates alapeatükkides antakse juhiseid, kuidas tööprotsesside mõjuanalüüsi üksikuid samme läbi viia. Vajaliku info kogumiseks võib kasutada küsimustikke, töökoosolekuid või individuaalseid vestlusi. Mõislik oleks nimetatud meetodeid omavahel kombineerida, kuna neil kõigil on oma eelised ja puudused ja nad täiendavad üksteist. Näiteks saab küsimustikke, olgu need paberil või tarkvarapõhiseid, sõnastada ainult üldise suunitlusega nõnda, et need kehtiksid korraga kõikide valdkondade ja tööprotsesside jaoks. Selleks, et tutvustada hädaolukordade halduse teemat ja näidata, miks ja millise eesmärgiga tuleb teatud samme kasutusele võtta, saab kasutada töökoosolekuid, kuhu kogutakse korraga kokku suurem hulk erinevate valdkondade töötajaid. Üksikvestlused osakonnajuhatajatega, protsesside eest vastutavatega või muude isikutega, kellel on olulist infot, nõuavad küll kõige rohkem aega, kuid annavad ka täpsemat infot, kuna vestluse juhtimise ja sobiva küsimustehnikaga on võimalik arusaamatusi tuvastada ja kõrvaldada ning seeläbi jõuda olulise teabeni.

Tööprotsesside mõjuanalüüs jaoks sobiva vestluspartneri valimine sõltub vastavast protsessisammust ning organisatsiooni ülesehitusest.

Tööprotsesside mõjuanalüüsi (BIA) läbiviimisel on määrava tähtsusega organisatsiooni juhtkonnalt saadav abi. Kuna oluline on laialdane koostöö erinevate ärivaldkondade, osakondade ja ressursside tasandi (nt IT-administreerimise) vahel, tuleks tagada, et vastava tööülesande jagamine käiks kõige kõrgema juhtimistasandi kaudu ja et kogu organisatsioon mõistaks selle ülesande olulisust.

5.1.2.1 algandmed ja äriprotsessid

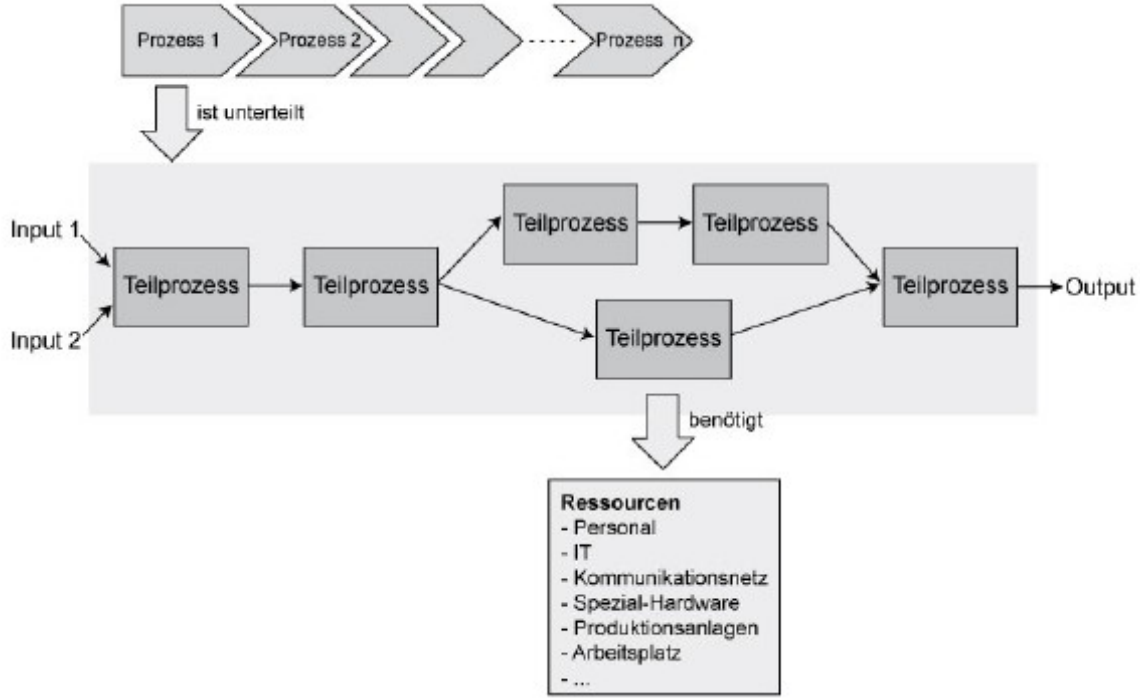
Tööprotsesside mõjuanalüüsi eelduseks on ärimudeli või organisatsiooni ülesannete ja nende ülesehituse põhjalik tundmine. Selle alla kuulub äriprotsesside ja erialaste ülesannete ning organisatsiooni algandmete tundmine. Algandmeteks on näiteks teave ettevõtlusvormi, valdkonna, töökorraldusliku struktuuri, asukohtade või tarnijate kohta. Ametiasutustes on äriprotsessideks nende tööülesanded. Kui edaspidi mainitakse äriprotsesse, siis mõeldakse nende all ka ametiasutuste tööülesandeid. Ühe mõiste kasutamine on vaid teksti parema loetavuse huvides.

Igal organisatsioonil peaks olema oma olulistest protsessidest täielik, värske ja hästi dokumenteeritud ülevaade. Kui ülevaade puudub, tuleb see koostada ning kui see on aegunud, tuleb seda uuendada. Ülevaate koostamine ei ole otseselt hädaolukordade halduse spetsiaalne ülesanne.

Ei ole olemas üheselt mõistetavaid ja üldkehtivaid andmeid selle kohta, mida tuleks äriprotsessi all mõista (vt joonis 4). Käesolev dokument lähtub järgnevast: väärtust loov ahel hõlmab toote või teenuse kogu teekonda alates tootjast kuni tarbijani ja ahelasse võib kuuluda mitu organisatsiooni. Väärtusteahela all mõistetakse väärtuseid loova ahela neid osasid, mis piirduvad ühe organisatsiooniga. See koosneb mitmest üksteisega seotud äriprotsessist (protsessiahel), reeglina alates tellimusest kuni tarnimise ja arveldamiseni. Äriprotsessi võib vaadelda osaprotsesside jadana, mis sisaldab erinevaid tegevusi ja otsuseid. Iga osaprotsess on omakorda äriprotsess. Protsess vajab tavaliselt teistest äriprotsessidest tulevat sisendit (input). Protsessi tagajärjel tekib mingi väljund (output), nt toode, info või teenus, mida saab kasutada järgmistes protsessides. Sisend ja väljund on protsesse ühendavad elemendid. Tööprotsesside mõjuanalüüsi tegemiseks on äriprotsesse kasulik võimalusel määratleda selliselt, et nad jääksid täielikult organisatsiooni ühe osakonna ja seega ühe vastutusala piiridesse.

Äriprotsesse liigitatakse tuumprotsessideks ja abiprotsessideks. Tuumprotsessid annavad ühe või mitme ärieesmärgi saavutamisse otsese panuse. Neid saab omakorda liigitada strateegilisteks protsesssideks, mis aitavad organisatsioonidel langetada strateegilisi otsuseid, ja operatiivseteks protsessideks, mis on osa igapäevasest äritegevusest. Operatiivseks äritegevuseks võib olla nt ametiasutusele suunatud riiklike ülesannete täitmine, teenuste osutamine või ka mõne toote tootmine.

Abiprotsessid ei osale vahetute ärieesmärkide täitmises, kuid nende kaudne mõju võib olla siiski väga oluline ja kriitilise tähtsusega, kuna nad peavad aitama tuumprotsesse käigus hoida. Klassikalisteks abiprotsessideks on personalihaldus ja infosüsteemide administreerimine.



Joonis 4. »Äriprotsessid

Input – sisend;
Prozess – protsess;
ist unterteilt – jaguneb omakorda;
Teilprozess – osaprotsess;
Output – väljund;
benötigt – vajadused;
Ressourcen – ressursid;
Personal – personal;
IT – IT;
Kommunikatsionsnetz – sidevõrk,
Spezial-Hardware – spetsiaalne riistvara;
Produktionsanlagen – tootmisseadmed;
Arbeitsplatz – töökoht

Protsessi ülevaate väljatöötamine eeldab nii terviklikku ülevaadet organisatsioonis toimuvast kui ka üksikute ülesannete tundmist. Üheks meetodiks, kuidas saavutada tuumprotsessidest täielik ülevaade, on vaadelda väärtusahelat alates tellimusest kuni tarnimise ja arveldamiseni. Mõistlik oleks see ülesanne delegeerida organisatsiooni vastavale osakonnale. Organisatsiooni erinevad osakonnad peaksid oma valdkonna äriprotsessidest ülevaate koostama. Ülevaate koostajateks võivad olla organisatsiooni osakonnajuhatajad, selleks nimetatud vastutavad töötajad või selle organisatsiooni vastava osakonna eest vastutav hädaolukorrakoordinaator. Hädaolukorrakoordinaator peaks äriprotsesse ja kontaktisikuid juba tundma, kuna ta vajab neid teadmisi hädaolukordade halduses.

Kui äriprotseduuride tuvastamine toimub hädaolukorraennetuse raames, peaks hädaolukorraametnik seda ülesannet informeerivalt, koordineerivalt ja juhtivalt toetama. Võrreldavate tulemuste saamiseks peaks ta määratlema andmete kogumismeetodid, protsesside kujutamisviisi ja detailsuse, samuti klassid ja ühtsed raamtingimused. Organisatsiooni osakonnad peavad neid nõudeid andmete kogumisel kasutama. Hädaolukorraametnik peab regulaarselt organisatsiooni eri osakondade andmetöötlejate tööd kooskõlastama, et protsesside kujutamisega seotud suuri erinevusi juba varakult avastada ja kõrvaldada. Ta koondab üksikud tulemused kokku ja konsolideerib need koostöös juhtkonnaga. Selle kõige tulemusel peaks tekkima protsessiskeem, milles loetletakse

protsessid ja näidatakse äriprotsesside omavahelisi erinevaid sõltuvussuhteid. Selle alla kuuluvad protsessi- ja väärtusteahelad ning toetatavate äriprotsesside sõltuvuslikud seosed.

Kui osad äriprotsessid, mis kuuluvad organisatsiooni väärtusteahelasse, on tellitud väljastpoolt, tuleb ka need protsessid ülevaatesse kaasata ja vastavalt tähistada. Oluline on näidata organisatsioonisiseseid äriprotsesse ja nende omavahelisi sõltuvussuhteid.

Protsesside määratlemise detailsuse puhul tuleks leida kuldne kesktee liiga tugeva üldistamise ja liiga detailse vaatlemise vahel. Protsesside liiga tugeva kokkukoondamise tagajärjeks on teabe madal väärtus. Liiga detailse vaatlemise tagajärjeks on vaadeldavate protsesside üleküllus. Praktilised kogemused on näidatud, et tööprotsesside mõjuanalüüsi koostamisel peaks üksikute äriprotsesside detailsus olema selline, et teatud rakenduste puhul oleks spetsiifiliste nõudmiste esitamine küll võimalik, kuid samas ei peaks see tähendama täielikku äriprotsesside analüüsi. Üldiseks rusikareegliks on, et protsessiinfo kogumine peaks organisatsiooni ühe osakonna raames hädaolukordade halduse jaoks välja tooma 5, maksimaalselt aga 15 protsessi. Sellised arvud on praktikas olnud kõige mõistlikumad, kuid institutsioon ja selle tegevusvaldkond võivad neid arve ka nt kahandada või suurendada.

Iga äriprotseduuri või selle osa kohta tuleb lisada vähemalt alljärgnev teave:
- protsessi selge nimetus,
- lühike kirjeldus,
- vajalik sisend,
- saadav kasu,
- osaprotseduurid juhul, kui on loodud alajaotusi,
- seosed teiste organisatsioonisiseste ning -väliste äriprotsessidega (eelmised ja järgmised lülid) ja seosed abiprotsessidega, nt infotehnoloogiateenustega,
- äriprotsesside sõltuvusaste (vt ptk 5.1.2.5) ja
- protsessi eest vastutav isik või protsessi kontaktisik.

Protsessi väljaselgitamiseks võib abivahenditena kasutada äriprotseduuride tarkvaralisi modelleerimisvahendeid.

5.1.2.2 protsessi kaasatavate allüksuste ja tööprotsesside valimine

Kui on selge, et hädaolukordade halduse kehtivusala piiridesse jäävad mõningad osakonnad või äriprotsessid, mis on organisatsiooni jaoks väga väikese tähtsusega, võib need edasisest vaatlusest kõrvale jätta. See aitab töövaeva ja kulutusi veidi vähendada. Siiski tuleb arvestada sellega, et teatud protsesside omavaheliste sõltuvussuhete olulisus pole alati selgelt nähtav ning neid seoseid võidakse alahinnata. Väljast tellitud protsessidele kehtivad samad reeglid. Väljast tellitud protsesse tohib ainult siis kõrvale jätta, kui neid saab selgelt ebakriitilisteks liigitada.
Kui organisatsioonis leidub osakondi, mille prioriteeti organisatsiooni juhtkond strateegilistel põhjustel teistest madalamaks hindab, võimaldab see vaadeldavate äriprotsesside mahtu veelgi vähendada. Sellele vaatamata on tegu otsusega, mida saab langetada vaid juhtkonna kõige kõrgem tasand.

Kui vaadeldava lõigu piiramist võimaldavat lähenemist rakendatakse kehtivusala piires, tuleb üksikute äriprotsesside või lausa organisatsiooni osakondade kõrvalejätmist kirjalikult ja ühetimõistetavalt põhjendada. Organisatsiooni juhtkond peab sellele piirangule oma loa andma ja selle allkirjaga kinnitama. Kõrvalejätmist tuleb BIA järgmise uuendamise raames põhjalikult kontrollida, et näha, kas argumentatsioon on osutunud õigeks.

5.1.2.3 Kahjude analüüs

Kahjude analüüsi abil uuritakse organisatsioonile tekkivaid kahjusid, mis võivad tekkida erinevate tööprotsesside katkemisel. Siinkohal ei ole oluline mitte üksnes kahju suurus, vaid

ka selle ajaline kestus. Kahjude analüüsi läbiviimiseks tuleb kindlaks määrata mitmed raamtingimused. Selle alla kuuluvad kahjude kategooriad, kahjude stsenaariumid, vaadeldavad hindamisperioodid ja spetsiaalsete tähtaegadega toimetulemise strateegia.

A. Kahjukategooriate ja -stsenaariumite kindlaksmääramine

Protsessi katkemisest tulenev kahju koosneb otsestest kahjudest (nt saamatajäänud tulu, õiguslikest tagajärgedest tulenevad kulutused) ja kaudsetest kahjudest (nt saamatajäänud tellimused, turuosa vähenemine, imidži kahjustumine). Kuna mainitud kahjustustest saab vaid osa konkreetsetes arvudes väljendada, on mõistlik kahjustusi mitte ainult kvantitatiivselt välja arvutada, vaid kasutada ka kahjukategooriate kvalitatiivset liigitamist. Iga organisatsioon peab kahjude kategooriate hulga ja tähenduse ise määratlema. Tavaliselt piirdutakse kolme kuni viie kategooriaga. Käesolevas dokumendis olevas näites jaotatakse see nelja kategooriasse (vt tabel 1). Kahjukategooriad on võrreldavad IT-etalonturbe vajalike turbeastmete tuvastamise [BSI2] kahjukategooriatega. Tabel 1 kajastab kahju- ja kaitsekategooriate vastandamist.

Kahjukategooriad		Kaitsevajaduse kategooriad	
Tähistus	Selgitus	Tähistus	Selgitus
Madal	Katkestuse mõju on väike, vaevutuntav		
Tavaline	Katkestuse mõju on tuntav.	Tavaline	Kahjude tagajärjed on piiratud ja neist on ülevaade.
Kõrge	Katkestuse mõju on selgelt märgatav.	Kõrge	Kahjude tagajärjed võivad olla ulatuslikud.
Väga kõrge	Katkestus või mõjutused võivad ohustada organisatsiooni kestmajäämist.	Väga kõrge	Kahjude tagajärjed võivad võtta eksistentsi ohustava, katastroofilise ulatuse.

Tabel 1. Kahju- ja kaitsekategooriad

Erinevaid kahjukategooriaid võiks põhimõtteliselt määratleda ja piirata ka eranditult otsese rahalise kahju alusel, siiski on mõistlik hindamisse kaasata ka teisi kahjustsenaariumeid. Mittemateriaalsed või kaudsed rahalised kahjud võivad, sõltuvalt valdkonnast ja organisatsioonist, olla suuremad kui otsesed rahalised kahjud. Praktiline kogemus on näidanud, et mõistlik on kasutada vajalikest turbeastmetest tuntud kahjustsenaariumeid:

- rahalised tagajärjed,
- tööülesannete täitmise piiramine,
- seaduste, eeskirjade ja lepingute rikkumine,
- negatiivsed sise- ning välismõjud (imidžikahjustused) ning
- isikliku puutumatuse rikkumine.

Vabalt valitavate kahjustsenaariumite teisteks näideteks on:

- puuduv haldus- või juhtinfo või
- töötajate motiveerituse langus.

Organisatsioon peab kindlaks määrama, milliseid kahjustsenaariumeid tuleks kasutada ja millised peaksid olema kahjustsenaariumite prioriteedid. Suurema osa ettevõtete jaoks on peamiseks kriteeriumiks rahalised tagajärjed, kuid teatud valdkondades, nt pankade või kindlustusfirmade puhul, võib ka imidži kahjustumine olla väga tõsine. Ametiasutustes võib esimesel kohal seista tööülesannete täitmine, selle järel imidži kahjustumine. Kahjustsenaariumeid võib vabalt valida, samuti võib määratleda uusi.

Selleks, et kahjukategooriaid üksteisest eraldada, tuleb kahjustsenaariumite alusel nende piirid organisatsiooni jaoks individuaalselt kindlaks määrata (vt tabel 2). Kui tööprotsesside

mõjuanalüüsi tegemisega koos määratakse ka vajalik turbeaste ja selles kasutatakse kahjustsenaariumite alamjaotusi, on võimalik ära kasutada järeldusi, mis saadakse vajaliku turbeastme määramisest. Sellega muutub töö hulk väiksemaks. Tabel 2 loetleb võimalikke stsenaariume ja kategooriaid, mida tuleb siiski iga organisatsiooni jaoks individuaalselt kohandada.

Kahjukategooria „madal”	
Rahalised tagajärjed	Märkimisväärsed mõjud puuduvad (nt kaod on väiksemad kui 5% käibest)
Tööülesannete täitmise piiramine	Märkimisväärsed mõjud puuduvad
Seaduste jms rikkumine	Märkimisväärsed mõjud puuduvad
Negatiivsed organisatsioonisisesed ja -välised mõjud	Märkimisväärsed mõjud puuduvad
Kahjukategooria „tavaline”	
Rahalised tagajärjed	Rahaline kahju on organisatsiooni jaoks vastuvõetav (nt kaod on väiksemad kui 5–20% käibest)
Tööülesannete täitmise piiramine	Mõju on töötajate jaoks vastuvõetav / saab eelistada muid tegevusi / lisatöö ei takista ülesannete täitmist oluliselt / probleem ei sega organisatsiooni teisi osakondi või lepingulisi partnereid tööülesannete täitmisel
Seaduste jms rikkumine	Seaduste ja eeskirjade rikkumine on väikeste tagajärgedega / rikkumisi märgatakse ainult organisatsiooni sees
Negatiivsed organisatsioonisisesed ja -välised mõjud	Tõrkeid/katkestusi märgatakse ainult erandjuhul ja kliendid ning äripartnerid peavad neid ebaoluliseks / see ei mõjuta klientide ja äripartnerite arvamust / üldine usaldusväärsus organisatsiooni suhtes ei saa kahjustada / turuosa kadu on mittemärgatav
Kahjukategooria „kõrge”	
Rahalised tagajärjed	Rahalised kaod on märkimisväärsed, kuid ei ohusta eksistentsi (nt kahju jääb alla 20–30% käibest)
Tööülesannete täitmise piiramine	Vastuvõetamatud katkestused/piirangud / töökvaliteedi vähenemine / tähtaegade mittetäitmine märgatakse ka väljaspool organisatsiooni / mahajäämuse tasategemiseks ei piisa tavalisest tööajast / organisatsiooni muude osakondade või lepinguliste partnerite töö on olulisel määral häiritud, ka seal tuleb puudujääke kõrvaldada / leppetrahvid jäävad vastuvõetavatesse piiridesse
Seaduste jms rikkumine	Seaduste ja ettekirjutuste rikkumine on vastuvõetavate tagajärgedega / rikkumisi märgatakse ka väljaspool organisatsiooni
Negatiivsed organisatsioonisisesed ja -välised mõjud	Kliendid ja äripartnerid märkavad tõrkeid/katkestusi selgelt ja ka vastavas valdkonnas märgatakse probleeme / mõne kliendi ja äripartneri jaoks on imidž ja usaldusväärsus osalt rikutud / imidži ja usaldusväärsuse kaod tuleb suure töövaevaga tasa teha / üksikud kliendid ja äripartnerid lõpetavad ärisuhted / turuosa märgatav kadu / kadusid saab piisava töövaevaga tasa teha

Kahjukategooria „väga kõrge”	
Rahalised tagajärjed	Rahaline kahju ohustab organisatsiooni eksistentsi (nt kui kadu on suurem kui 30% käibest)
Tööülesannete täitmise piiramine	Tööülesannete täitmine on väga tõsiselt takistatud / mahajäämuse tasategemine on võimalik ainult välise abiga või üldse võimatu / hilinenud ja puudulikud tulemused on väljapoole selgelt märgata / teenuse kvaliteedi raskekujuline vähenemine / organisatsiooni teiste osakondade või lepingupartnerite töö on võimatu / kõrged kahjutasunõuded/leppetrahvid
Seaduste jms rikkumine	Seaduste rikkumine, millel on tagajärjed nii ärile kui ka töötajatele
Negatiivsed organisatsioonisisesed ja -välised mõjud	Suur osa kliente ja äripartnereid lasevad ennast juhtunust mõjutada / organisatsiooni imidž ja usaldusväärsus on tugevalt kahjustatud ja kahtluse alla seatud / imidži ja usaldusväärsuse taastamine on väga raske või võimatu / tugev turuosa kaotus / kahjude tasakaalustamine on väga raske või võimatu.

Tabel 2. Kahjukategooriate piiritlemise näide

Pärast seda, kui on kindlaks määratud, milliseid kahjukategooriaid hakatakse hindamisel kasutama, saab stsenaariumeid edasi analüüsida, vaadeldes nende olulisust institutsiooni jaoks. Olulisema suuna valimine on mõistlik sel juhul, kui kahjustsenaariumid „rahalised tagajärjed”, „tööülesannete täitmise piiramine”, „seaduste ja lepingute rikkumine”, „eluohtlik olukord” ja „negatiivsed organisatsioonisisesed- ja välised mõjud” on organisatsioonile erineva tähtsusega ja mõni nendest on tähtsam kui teine.

B. Vaadeldavate hindamisperioodide kindlaksmääramine

Erinevalt vajaliku turbeastme kindlaksmääramisest ei analüüsita tööprotsesside analüüsi käigus mitte ainult seda, milline oleks protsessi katkemise mõju organisatsioonile, vaid ka seda, milline on kahju ajaline areng. See eeldab niinimetatud hindamisperioodide kindlaksmääramist. Iga hindamisperioodi kohta koostatakse liigitus - kuidas mõjutab katkestusest tulenev kahju vastavat äriprotsessi -, tuues välja perioodi kahjukategooria.

Hindamisperioodide arv ja pikkus sõltub organisatsioonist, kuna need on olulisel määral seotud konkreetsete tingimustega. Nendeks tingimusteks võivad olla nt pakutud teenuste liik, äriprotsesside mitmekülgsus, toodete liik või lihtsalt tegevusvaldkond ja sellega seotud seadustest tulenevad ettekirjutused. Kui organisatsiooniks on nt pangaasutus, valitakse ilmselt väga lühikesed hindamisperioodid, samas kui ajalises mõttes vähemkriitilise ärimudeliga organisatsioon võib valida oluliselt pikemad perioodid. Hindamisperioodide arvu ja kestuse määramise kergendamiseks saab kasutada äriprotsesside taastamisklasse (vt ptk 5.1.2.6), eeldusel, et need on olemas ja nende seoseid on võimalik hinnata.

Keskmiste käideldavusnõuetega organisatsioonid on tavaliselt valinud neli kuni kümme hindamisperioodi. Alljärgnevas tabelis on toodud hindamisperioodide jaotamise erinevaid näiteid. Ajalised andmed tähendavad järgneval juhul „kuni ... tundi”.

	Hindamisperioodid (96 tundi = 4 päeva, 168 tundi = 1 nädal, 720 tundi = 1 kuu)									
Ajaperiood	1	2	3	4	5	6	7	8	9	10
Näide nr 1	24	72	240	720						
Näide nr 2	8	24	48	72	168	720				
Näide nr 3	1	2	4	8	24	48	96	168	240	720

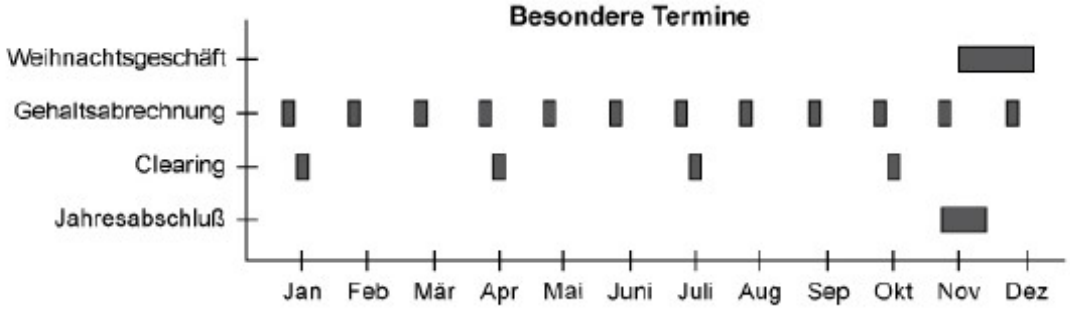
Tabel 3. Hindamisperioodide näited

Vajadusel võib lisada veel ühe täiendava hindamisperioodi, nt „>3 kuud", mis sobib olukorras, kus infrastruktuur on tõsiselt kahjustada saanud või on asukoht kahjustada saanud ja puuduvad asendustöökoha kasutamise plaanid. Kui ümberasumist võimaldavad asukohad ning vastavad ennetusmeetmed puuduvad, kulub taastamismeetmetele, alustades kõigepealt uue asukoha otsingust, väga kaua aega.

C. Spetsiaalsed tähtajad ja sündmused

Paljude äriprotsesside käideldavusnõuded võivad päevade, kuude või aastate kaupa oluliselt erineda. Selle põhjuseks võivad olla kindlad ajaintervallid (nt igapäevane tööpäeva või töövahetuse lõpp pangas, iganädalase ajalehe kuulutuste trükkiandmise tähtaeg, raamatupidamise aastaaruande lõpptähtaeg, jõulueelne aeg internetipoes (või teatud nädalapäev iganädalase ajalehe väljaandja jaoks) või teatud sündmused (nt panga intressimäära tõstmine või jalgpalliülekande paus veepuhastusjaama jaoks).

Iga organisatsioon peab langetama strateegilise otsuse selle kohta, kuidas neid hooajalisi või sündmustest tingitud käideldavuse mõjusid kahjuanalüüsis käsitleda, ning selle otsuse dokumenteerima. Sel põhjusel, samuti strateegiliste otsuste baasi loomiseks, tuleks need tähtajad koos võimalike sündmuste ning esinemistõenäosustega kirja panna ning anda umbkaudne hinnang vastavate protsesside käideldavusnõuete kõikumiste kohta. Spetsiaalsetest tähtaegadest saab luua hea ülevaate kalendri vormis (vt joonis 5). Erilised sündmused, mille esinemist ei saa ajaliselt ette ennustada, tuleb eraldi kirja panna.



Joonis 5. Spetsiaalsed tähtajad

Besondere Termine – spetsiaalsed tähtajad;
Weichnachtsgeschäft – jõuludega seotud ettevõtlus;
Gehaltsabrechnung – palkade arvestamine;
Clearing – tasaarveldus;
Jahresabschluss – aasta lõpp

Spetsiaalsete tähtaegade ja sündmuste teadmine võib olla olulise tähtsusega teave, mis aitab hädaolukorraolukorra likvideerimise käigus otsuseid langetada. Lisaks on sellisest teadmisest abi ka testide ja õppuste planeerimisel ja kinnitamisel. Teste ja õppuseid ei tohiks planeerida aegadele, mil valitsevad kõrged käideldavusnõuded.

Spetsiaalsete tähtaegade ja sündmustega toimetulemise strateegia võimalikud variandid on järgmised:
- Kahjuanalüüsi aluseks võetakse Worst-Case stsenaarium, ehk vastava äriprotsessi spetsiaalsetel tähtaegadel ja sündmustel põhinev kõige kõrgem käideldavusnõue, mis kantakse üle tervele ajavahemikule.

- Kahjude analüüsi puhul eristatakse vaadeldavate protsesside erinevaid ajavahemikke ja iga ajavahemiku jaoks vajalik teave kogutakse eraldi.
- Kahjude analüüsi aluseks on tavaolukord.

Esimene võimalus, mida kasutatakse praktikas kõige sagedamini, tähendab suuremat ennetamise töömahtu, kuid nagu Murphy seaduski ütleb: „Kui midagi saab viltu minna, siis ta ka läheb," ning seetõttu tuleb arvestada, et hädaolukorda tekib alati kõige ebasoodsamal hetkel. Teine variant tähendab tööprotsesside mõjuanalüüsi, prioriteetide kehtestamise, hädaolukorraplaanide väljatöötamise ning testide ja õppuste läbiviimisega seoses suurendatud töömahtusid. Kui eristatavate ajavahemike arv on suur, suureneb tööde hulk teise variandi puhul väga järsult, ning seetõttu tuleks seda varianti kasutada ainult siis, kui ajavahemike hulk on väga väike. Kolmas variant tähendab teadlikku arvestamist, et spetsiaalsetele tähtaegadele ja ajavahemikele kehtib teatud risk, kuid seda tuleks kasutada ainult erandjuhtudel. See variant võib olla mõistlik juhul, kui kõrgemaid nõudeid tagavate ennetavate meetmete rakendamisele kuluv aeg ja vaev ei ole riskiga mõistlikus tasakaalus, kuna kõrgemate nõuete eiramisel jääb riski tekkimise võimalus väga väiksesse ajavahemikku. Selle variandi valimisel tuleb lisaks valitud strateegia dokumenteerimisele ka selgelt ja mõistetavalt ära näidata võimalik risk ning põhjendada, miks otsustati just sellise lähenemise kasuks. Juhtkond peab riski teadvustamist kirjalikult kinnitama.

D. Kahjude analüüsi tegemine

Pärast seda, kui eeltööd on tehtud ja raamtingimused kindlaks määratud, võib alata tegelik kahjude analüüsimine. Selleks tuleb nüüd iga erineva äriprotsessi puhul hinnata, milline on protsessi katkemise mõju organisatsioonile, tuues välja erinevad hindamisperioodid ja kahjustsenaariumid, st kahjude ajaline kulg tuleb tuvastada.

Kahjude analüüsi peaksid tegema organisatsiooni erinevad osakonnad, kuna see eeldab äriprotsesside põhjalikku tundmist. Hädaolukorrakoordinaatorid vastutavad analüüsi teostamise eest ja töötlevad kogutavat infot koos protsessi eest vastutava isikuga ja vajadusel ka koos osakonnajuhatajaga.

Hinnang võib olla järgnev: „Protsessi katkemisega kaasneksid otsesed majanduslikud kahjud, mis on kuni 96 tunni jooksul madalad, kuni 168 tunni jooksul tavalised ja alates 720 tunnist kõrged, samal ajal pole seadusega vastuollu minemise ohtu". Praktikas kasutatakse sageli tabelit, mille eeliseks on kiire ülevaade. Tabelis 4 on ära toodud lihtsustatud näide sellest, milline võib protsessi kahjude analüüs tabeli kujul välja näha.

Äriprotsessi kahjude ajalise kulgemise hindamiseks võib kindlaks määrata kaalutud summad, lähtudes kahjude stsenaariumitest või ajast (tabeli 4 viimane rida). Summad näitavad kõikide üksikute vaatlusperioodide kõikide kaalutud kahjustsenaariumite vastavat kogukahju.

Protsess: protsessi nimi										
Andmetöötleja: hr Jaakson (hädaolukorrakoordinaator)										
Kontaktisik / intervjueeritav: pr Ilves (protsessi eest vastutav)										
Organisatsiooni allüksus: osakond nr 1										
Koostamise kuupäev: 11. veebruar 2008										
Ajavahemik:										
Taaskäivitamine:			Taastamine:			Maksimaalselt vastuvõetav katkestusaeg:				
Taaskäivitamise tase:										
Hindamisperioodid Kahjustsenaariumid		8 tundi	24 tundi	48 tundi	96 tundi	168 tundi	720 tundi	>720	kaal	Märkused
Rahalised tagajärjed	1	1	1	2	2	3	3	3		
Tööülesannete täitmise piiramine	1	1	2	2	3	3	4	4		
Seaduste, lepingute		ei rakendu sellele								

rikkumine		protsessile							
Imidži kahjustumine	1	1	1	1	1	2	3		
Kaalutud ∑	9	9	12	17	20	26	30		

Tabel 4. Äriprotsessi kahjude ajalise kulgemise näide (1 = madal, 2 = tavaline, 3 = kõrge, 4 = väga kõrge)

Kui rahaliste tagajärgede puhul on eeldatava kahju kohta olemas täpsem info (nt juhtimisarvestuse abil leitud andmed), saab ka need tabelisse üle võtta. Täpsete summade kirjapanek eeldab täpsust, mis pole sageli saavutatav, seega tuleks seda vahendit kasutada ainult siis, kui summad on õiged ja realistlikud. See võib olla kvalitatiivse hindamise jaoks kasulik lisateave.

Üks võimalus, kuidas äriprotsessidest head ülevaadet saada, on üksikute protsesside tulemuste koondamine tervikülevaatesse. Tabelid 5 ja 6 on toodud näideteks, kuidas saab kahel erineval moel kujutada äriprotsesside kahjude ajalist kulgemist. Ülevaatlikuma näite saavutamiseks on kahjude stsenaariumeid ja hindamisperioodide arvu vähendatud.

				Rahaline tagajärg				Tööülesannete täitmise piiramine				Negatiivsed organisatsioonisisesed ja -välised mõjud			
				Raskusaste: 5				Raskusaste: 3				Raskusaste: 1			
Protsessid	Taas-käivitamine	taastamine	katkestusmax vastuv.	24 tundi	48 tundi	96 tundi	192 tundi	24 tundi	48 tundi	96 tundi	192 tundi	24 tundi	48 tundi	96 tundi	192 tundi
P1				1	1	3	4	1	1	2	3	1	1	1	2
P2				1	2	3	4	1	2	3	3	1	1	2	3
P3				1	1	1	2	1	2	3	3	1	2	3	4
...															
P12				1	1	2	4	1	2	3	3	1	1	1	1

Tabel 5. Kahjude hindamise ülevaate näide nr 1

Prozess	Wiederanlauf	Wiederherstellung	Max. tol. Ausfall	24 Stunden	48 Stunden	96 Stunden	192 Stunden	Gewicht	Schadensszenario
P1				1	1	3			
				1	1	2			
				1	1	1	2		Imageschaden
				9	*9*	*22*	*31*		*Gew. Σ*
P2						3	4	5	finanzielle Auswirkungen
						3	3	3	Beeintr. der Aufgabenerfüllung
				1	1	2	3	1	Imageschaden
				9	*17*	*26*	*32*		*Gew. Σ*
P3				1	1	1	2	5	finanzielle Auswirkungen
				1	2	3	3	3	Beeintr. der Aufgabenerfüllung
				1	2	3	4	1	Imageschaden
				9	*13*	*17*	*23*		*Gew. Σ*
…	…		…	…	…	…	…	…	…
P12				1	1	2	4	5	finanzielle Auswirkungen
				1	2	3	3	3	Beeintr. der Aufgabenerfüllung
				1	1	1	1	1	Imageschaden
				9	*12*	*20*	*30*		*Gew. Σ*

Gewichteter Schaden nach 192 Stunden

Schadensanstieg

Tabel 6. »Kahjude hindamise ülevaate näide nr 2
Prozess – protsess;
Wiederanalauf – taaskäivitamine;
Wiederherstellung – taastamine;
Max. tol. Ausfall – max vastuvõetav katkestus;
Stunden – tundi;
Gewicht – raskus;
Schadensszenario – kahjustsenaarium;
Gewichteter Schaden nach 192 Stunden - kaalutud kahju 192 tunni möödudes;
finanzielle Auswirkungen - rahalised tagajärjed;
Beeintr. der Aufgabenerfüllung - tööülesannete täitmise piiramine;
Imageschaden – imidži kahjustumine;
Gew. ∑ – kaalutud tulemus

Protsesside taaskäivitamise ja taastamise aegade kindlaksmääramisel tuleks arvestada nii kahju ajalise kulgemisega, kahjuga teatud ajavahemiku möödudes (nt kaalutud kahju 192 tunni möödudes vastavalt tabeli nr 6 näitele), kui ka taaskäivitamise/taastamise jaoks olemasoleva jõudlusega. Seejuures võib lähtuda nii kahju suurenemisest kõikide kahjustsenaariumite puhul kui ka vastavast kogukahjust.

Hädaolukorraametnik liidab organisatsiooni erinevate allüksuste kahjude analüüsi kokku ning konsolideerib andmed.

Selle, milline on kahjude analüüsi meetod ja detailsus, peab iga organisatsioon ise otsustama. Väikese või keskmise suurusega organisatsioon võib hindamisperioodide ja kahjude stsenaariumite arvu vähendada ja kasutada kirjeldatud meetodit. Väikese organisatsiooni pragmaatiline lähenemine, mis ei taga küll ei täielikkust ega ka objektiivselt kontrollitavaid tulemusi, oleks nt see, et olulised protsessid selgitatakse välja, jagatakse klassidesse ja pannakse töökoosoleku raames prioriteetide järjekorda. Samas tehtaks koostööd puudutatud protsesside eest vastutavate töötajatega. Minimaalseks nõudeks on äriprotsesside nimekirja koostamine ja nende käideldavusnõuete kindlaksmääramine. Kui turvakontseptsioon on BSI standardi 100-2 alusel juba koostatud, on suur osa ressursse kajastavast teabest juba olemas ja seda saab ära kasutada.

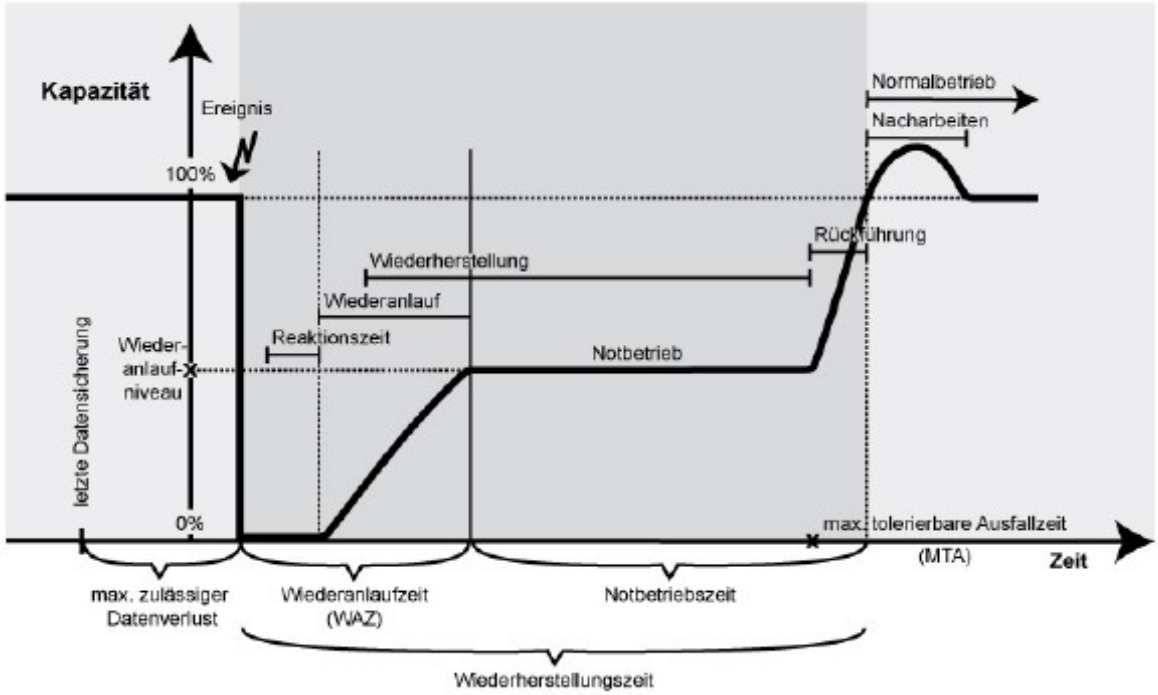
5.1.2.4 Taaskäivitamisparameetrite määratlemine

Kahjude analüüsi läbiviimise ajal või ka pärast seda tuleb määrata maksimaalne vastuvõetav katkestusaeg, taaskäivitamise aeg ja erinevate äriprotsesside taaskäivitamise tase.

Protsessi maksimaalne vastuvõetav katkestusaeg (ingl Maximum Tolerable Period of Disruption, MTPD) tähistab aega, mille jooksul peab toimuma taaskäivitamine, et organisatsioon ei satuks olukorda, mis ohustaks selle eksistentsi kas lähemas või kaugemas tulevikus. Taaskäivitamise aeg (ingl Recovery Time Objective, RTO) on eesmärgiks seatud aeg, mille jooksul peaks protsessi taas käivitama. Taaskäivitamise aeg peab olema lühem kui maksimaalne vastuvõetav katkestusaeg.

Protsessi taaskäivitamine, mida nimetatakse ka töö jätkamiseks, võib toimuda:
- hädaolukorrarežiimis, vähendades jõudlust ja ressursse, seda nii tavapärases töökeskkonnas kui ka
- alternatiivressursside abil (nt mõnes alternatiivses asukohas), samuti
- alternatiivprotsessina, kasutades teisi ressursse ja töömeetodeid.

Lisaks taaskäivitamise ajale tuleb määrata ka taaskäivitamise tase ehk stabiilse hädaolukorrarežiimi jaoks vajalik protsessijõudlus (nt 60% tavajõudlusest).



Joonis 6. Taaskäivitamise parameetrid

Kapazität – jõudlus;
Ereignis – sündmus;
letzte Datensicherung – viimane andmevarundus;
Wiederanlaufniveau – taastamise nivoo;
max. zulässiger Datenverlust – max vastuvõetav andmekadu;
Wiederanlaufzeit – taaskäivitamise aeg;
Notbetriebszeit – hädaolukorrarežiimi aeg;
Wiederherseellungszeit – taastamise aeg;
max. tolerierbarer Ausfallzeit – max vastuvõetav katkestuse aeg;
Wiederherstellung – taastamine;
Wiederanlauf – taaskäivitamine;
Reaktionszeit – reageerimisaeg;
Notbetrieb – hädaolukorrarežiim;
Normalbetrieb – tavarežiim;

Nacharbeiten – järeltööd;
Rückführung – tavaolukorra taastamine;
Zeit – aeg

Hädaolukorra ajalise kulgemise ja protsessi taaskäivitamise vaatlemisel on mõistlik vaadelda, kindlaks määrata või kaasata ka teisi tegevusi ja nende vajalikke ajavahemikke (vt joonis 6). Taaskäivitamise aeg koosneb hädaolukorra avastamiseni kulunud ajast (alates teavitamisest ja eskalatsioonist kuni taaskäivitamise meetmete rakendamiseni) ja reaalse taaskäivitamise ajast. Kuna taaskäivitamine toimub tavatöö käigus vaid harva, on mõistlik kindlaks määrata maksimaalne vastuvõetav hädaolukorrarežiimil toimuva töö aeg või maksimaalne vastuvõetav taastamisaeg. Viimane on taaskäivitamise aja ja maksimaalse vastuvõetava hädaolukorrarežiimil toimuva töö aja summa.

Taastamisaeg võib olla ka pikem kui maksimaalne vastuvõetav katkestusaeg, kuna hädaolukorrarežiimis toimuv töö lükkab eksistentsi ohustava olukorra saabumist edasi. Hädaolukorrarežiimilt tavarežiimile tagasiliikumise aeg on osa hädaolukorrarežiimis toimuva töö ajast ja sellega tuleb planeerimisel arvestada. Kui tavarežiim on taastatud, tuleb võib-olla teha vajalikud järeltööd, mis võivad vajada täiendavat aega – need tuleb arvestada tavarežiimi aja hulka. Maksimaalselt vastuvõetava hädaolukorrarežiimi määratlemisel tuleks vaadelda ka sellest tulenevat järeltööle kuluvat aega. Kui järeltööle kuluv aeg muutub liiga kaua kestva hädaolukorrarežiimi tõttu nii mahukaks, et seda pole võimalik normaalse aja jooksul ära teha, võib sellest tekkida järgmine kriis.

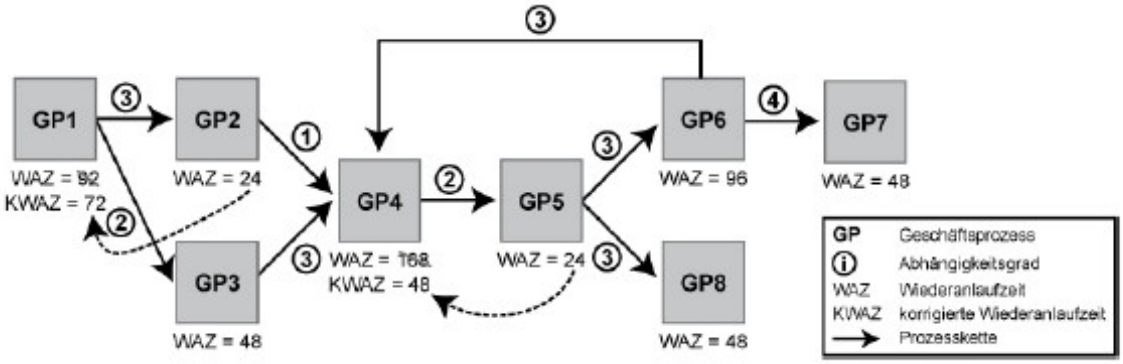
5.1.2.5 Sõltuvussuhetega arvestamine

Kahjude analüüs ning maksimaalselt vastuvõetav katkestuse aeg, taaskäivitamise aeg ja võimalik taastusperiood sõltuvad üksikprotsessidest. Järgmise sammuna tuleb arvestada omavahelise sõltuvusega äriprotsesse ning vajadusel käideldavuse ja kättesaadavuse nõudeid korrigeerida. Võimalusel tuleks protsesside taaskäivitamise prioriteetide määramisel arvestada lisaks ka asutuse või ettevõtte strateegiliste sihtidega (*Top down*-meetod).

Protsessisõltuvus

Erinevate äriprotsesside vaheline sõltuvus võib tähendada, et erinevate üksikute protsesside taaskäivitumise ajad tuleb omavahel sobitada. Paranduste ulatuslikkus sõltub protsessidevahelise sõltuvuse tasemest. Kui äriprotsess vajab väljundit (*Output*) või mõne teise protsessi teenuseid, siis kantakse kõrgem käitlemisvajadus nõrgendatud kujul teenindavatele protsessidele üle. Kui protsess genereerib väljundi, tuleb välja selgitada, kuivõrd on vajalik, et genereeritud väljund järgmises protsessis kohe ära tarbitaks. Sellisel juhul tuleb kõrgem kättesaadavusaste anda edasi ka järgnevale protsessile, mis kindlustab, et protsessijadas ei tekiks „ummistusi", kuna väljundit ei ole võimalik edasi anda. Protsesside sõltuvuse analüüsi tuleb sisse arvestada ka väljastpoolt tellitud protsessid (*outsourcing*).

Edasiandmise aste ja sellega seotud protsessi taaskäivitusaeg sõltuvad protsessi sõltuvuse astmest. See tähendab, et mida suurem on protsesside vaheline sõltuvus, seda tugevam on taaskäivitumise aja suurendamine või tasakaalustamine. Seetõttu ei ole mõttekas eristada ainult „sõltumatust" ja „sõltuvust", vaid valida tuleks astmeline sõltuvusmudel. Sõltuvustaseme määramiseks on soovitatav kasutada 3-6 astmelist mudelit. Näide 4. sõltuvusastmega võiks välja näha järgmiselt: 1=,väga kõrge, 2=,kõrge, 3=,keskmine, ja 4=,madal. ,Madal sõltuvustase tähendab, et kohandamist ei ole vaja, ning ,väga kõrge sõltuvustase tähendab taaskäivitamise aegade üks ühele ülevõtmist. Vaheastmetele tuleks sõltuvusastme definitsioon iseseisvalt määratleda. Joonisel 7 on näidatud tegevuse lihtsustatud kuju. Näiteks kuna protsesside GP5 ja GP4 vahel on kõrge sõltuvus, laiendatakse GP5 taaskäivituse aeg ka protsessile GP4. Seeläbi vähendatakse GP4 taaskäivitumise aega 168 tunnilt 48 tunnile. Peale taaskäivitumisaja peaks kontrollima ka üksteisest sõltuvate protsesside taaskäivitumise taset ning vajadusel neid ka ühtlustada.



Joonis 7: Taaskäivitusaja edasiandmine eelnevale protsessile

GP- äriprotsess

I – Sõtuvusaste

WAZ – Taaskäivitusaeg

KWAZ – Korrigeeritud taaskäivitusaeg

⟶ – Protsessijada

Sõltuvusaste tuleb välja selgitada mõlemas suunas, nii eelneva kui ka järgneva protsessi suunas. Lähtuvalt protsesside iseärasustest tuleks kindlaks määrata sõltuvuse aste eelneva ja järgneva protsessiga. Mõttekas oleks seda teha tööprotsesside mõjuanalüüsi (BIA) raames protsessikaardi koostamisel.

Sõltuvusastme tase võib tava- või hädaolukorrarežiimis olla erinev. Kui selles kontseptsioonifaasis selgub, et esineb erinevusi ja on teada, kuidas hädaolukorrarežiim välja näeb, siis tuleks vaadelda sõltuvussuhteid hädaolukorrarežiimis. Kui hädaolukorrarežiimi tüüpi muudetakse või kinnitatakse kontseptsiooni käigus alles hilisemal ajahetkel, tuleks uuesti läbi viia vastav sõltuvuskontroll ja vajadusel teha korrektuure.

Protsessijadad

Kahjude analüüsi korral vaadeldi üksikuid äriprotsesse ja kahjuteket nende katkestuse korral. Protsessisõltuvuse vaatlemisel edastati kättesaadavusnõue mööda protsessijada sõltuvalt sõltuvusastmest. Põhimõtteliselt võib protsessijadasiseste kõrgete sõltuvuste korral olla mõttekas vaadelda neid ühe tervikuna ja kokku liita üksikute äriprotsesside kahju, mis kogu jada või ainult kindla osa rivist väljalangemisel tekiks. Kui kogukahju saavutab protsessijada katkemisel väga ruttu eksistentsi ohustavad mõõtmed, tuleb kontrollida, kas ei oleks mõttekas selle jada üksikuid taaskäivitusaegu allapoole korrigeerida.

Ärieesmärgid

Esmalt on mõttekas institutsioonijuhtimise kaudu sisse tuua *Top down*-meetod, mille korral vaadeldakse ärieesmärke, erinevate huvigruppide kavatsusi ja tuumprotsesse veel ühe vaatenurga alt. Asutuse ärieesmärgid tulenevad enamasti selle õiguslikust ülesandest. Juhatuse tasandil ei ole mitte ainult aktuaalset teavet institutsiooni suunitlusest, vaid ka teave tulevikustrateegiate ning nendega seotud üksikute äriprotsesside, äriharude, osakondade või isegi ettevõtte osade olulisuse ja tähtsuse kohta institutsioonile.

Top down-meetodiga lisahinnangu saamiseks määrab juhtkond huvigruppide, ärieesmärkide ja protsessijadade prioriteedid ning sellega koos ärieesmärgid, mis nende saavutamisele kaasa aitavad. Protsesse, mis on vajalikud kõrgema prioriteediga ärieesmärkide saavutamiseks, hinnatakse kõrgemalt kui näiteks protsesse, mis on vajalikud mõne vähemtähtsa ärieesmärgi saavutamiseks. Juhtimistasandi lisaaruanne lisatakse protsesside ja taaskäivitusaegade üldaruandele.

Selle põhimõtte järgimisel tuleks järgida kahte aspekti:

- kui üks protsess on mitme protsessijada osa, siis mõjutab see asjaolu kaudselt ka kahjude analüüsi,
- kuna vaadeldakse ainult protsesse, mis on otseselt seotud ärieesmärkide saavutamisega, siis vaadeldakse ainult tuumprotsesse. Toetavad äriprotsessid on sellest vaatlusest välja jäetud.

Ressursisõltuvus

Taaskäivitusaegade äriprotsessidele määramisel tuleks arvestada ka ressurssidega, mida vajatakse protsesside taastamiseks ja taaskäivitamiseks. Näiteks on mingil hetkel vaja paljusid protsesse korraga taaskäivitada, kuid olemasoleva personaliga ei ole saa seda teha. Sellest lähtuvalt võib olla vajalik taaskäivituse tasandus ja taaskäivitusaegade korrektuur.

Eriliste tähtaegade ja sündmuste järgimine

Kui eriliste tähtaegade käsitlemiseks valiti strateegia (vt peatükk 5.1.2.3.C), mille korral eristatakse erinevate protsesside juures vaadeldavaid ajavahemikke ning kahjude analüüsis tuuakse iga ajavahemiku jaoks eraldi välja vajalik informatsioon, tuleb need äriprotsessid prioriteetide määramisel eriti esile tõsta. Erinevate ajavahemike eristamine tähendab rohkem tööd nii protsessisõltuvuste edasiandmisel kui ka erinevatele ajavahemikele erinevate prioriteedinimekirjade koostamisel.

5.1.2.6 Äriprotsesside prioriteetide ja kriitilisuse määratlemine

Kui äriprotsesside taaskäivitusajad on kindlaks määratud ja kohandatud, siis on olemas ka järjekord, st prioriteetide asetus. Üldjuhul võib taaskäivitusaegu jagada taaskäivitusklassideks. Üksikutes klassides on võimalik veel omakorda määrata protsesside taaskäivitamise järjekord.

Järgneva kontseptsiooni tarvis ei ole vaja kriitilisust määrata, kuid see lihtsustab kommunikatsiooni. Äriprotsesside kriitilisuse määramisel võib kasutada taaskäivitusaega või taaskäivitusklassi, kuna kriisihalduses tähendab „kriitilisus" ajalises mõttes kriitilist. Kaudselt tähendab „kriitilisus" ka „kahjukriitilisust", sest mida kiiremini kahju suureneb, seda kiiremini peab protsessid taas käivitama. Kriitilisuse määramiseks võib peale taaskäivituse kasutada ka teisi kohaseid kriteeriume, näiteks maksimaalselt vastuvõetav katkestusaeg või kogukahju pärast x tunni möödumist. Iga institutsioon otsustab ise, mis on tema jaoks kriitiline ning milliseid kriisikategooriaid ja kui palju kasutatakse. Tabel 7 näitab nelja kriisikategooria ja kindlaks määramisvõimalusega näidet. Arvud on fiktiivsed ja seega ei sobi neid otse üle võtta.

Kriitilisuse kategooria	**Taaskäivitus**	**Maksimaalne vastuvõetav katkestusaeg**	**Kogukahju x tunni järel**	**Üldine**
„ei ole kriitiline"	> 720 tundi	> 504 tundi	„madal"	Katkestusel ei ole mõju või on ainult minimaalne mõju.
„vähe kriitiline"	< 720 tundi	< 504 tundi	„tavaline"	Katkestusel on mõju.
„kriitiline"	< 168 tundi	< 240 tundi	„kõrge"	Katkestusel on suur mõju.
„väga kriitiline"	< 4 tundi	< 6 tundi	„väga kõrge"	Katkestus või selle mõjud viivad eksistentsi ohustavate mõjudeni

Tabel 7: Näide kriitilisuse kategooriate kohta

Et järgnevate sammudena tehtavad jõupingutused jääksid mõttekuse piiridesse, määratakse kriitilisuse kategooriad nii, et kriisihalduse järgmised tegevused keskenduksid äriprotsessidele, millele on määratud vähemalt kriitiline tase. Järgnevas tekstis mõeldakse „kriitiliste" äriprotsesside all äriprotsesse, mis ei ole hädaolukorraks valmisoleku mõttes saanud madalat aja- või kahjukriitilist prioriteeti. See sõltub vastava institutsiooni hädaolukorra strateegiast

5.1.2.7 Tava- ja hädaolukorrarežiimiks vajalike ressursside väljaselgitamine

Äriprotsesside läbiviimiseks on vaja hulgaliselt ressursse. Kriitiliste äriprotsesside suhtes selgitatakse välja, milliseid ressursse vajatakse tavarežiimi ajal ning milliseid kasutatakse ainult ühes kindlas või mitmes protsessis. See informatsioon on taaskäivitusplaanide koostamisel olulise tähtsusega ning seetõttu tuleks andmete kogumisel olla äärmiselt tähelepanelik. Kui infosüsteemide etalonturbe järgi on olemas turvakontsept, siis on võimalik suur osa vajalikust informatsioonist antud struktuurianalüüsist üle võtta. Kuna kriisihaldusele pakuvad huvi erinevad ressursside klassid, siis tuleb ressursside kohta koguda veel lisateavet. Vaadeldavate ressursside hulka kuuluvad järgmised.

- Personal

  Äriprotsesside läbiviimiseks on vaja töötajaid, kes teevad otsuseid, opereerivad masinaid, sisestavad andmeid või teevad teisi ülesandeid. Kui mõne äriprotsessi tarvis vajatakse spetsiaalseid kvalifikatsioone või teadmisi, tuleks ka see üles märkida ning lisaks tuleks veel üles märkida olemasolevad, võimalikud või puuduvad asendajad. Kui taaskäivitamiseks või taastamiseks vajatakse spetsialiste, siis tuleks esitada ka see teave.

- Informatsioon
Informatsiooni hulka loetakse nii elektroonilisi andmeid kui ka paberkandjal dokumente, mida äriprotsesside teostamiseks vajatakse. Järgneva analüüsi jaoks on abiks äriprotsesside andmete tähenduse üldine liigitamine ning protsesside jaoks oluliste andmete tuvastamine.

Ressursiteabe kogumisel tuleks välja selgitada vähemalt kriitiliste andmete maksimaalselt vastuvõetav andmekadu (näiteks tehingute arv või andmete vanus). See väärtus mõjutab eelkõige andmevarundusstrateegiat.

- Informatsioonitehnoloogia
IT all mõeldakse näiteks rakendusi, riistvara, tarkvara, sideühendusi (nt intranet ja internet), aga ka keskjaamu, faksiseadmeid või skannereid.

- Spetsiaalsed seadmed ja rajatised
Spetsiaalsete rajatiste hulka kuuluvad muuhulgas tootmiskompleksid, turvalüüsid, meditsiinilised
seadmed ja juhtelemendid.

- Teenused
Esitada tuleb vajalikud sisemised või välised teenused, mis annavad sisendi või võimaldavad protsessi tööks vajalikke ressursse. Siseteenuse näiteks võiks olla IT-haldus.

- Infrastruktuur
Infrastruktuuri alla kuuluvad näiteks maa-ala, hooned, ladu, tootmishooned, garaažid, arhiivid, serveri- ja bürooruumid, töökoht, aga ka väline voolu-, gaasi-, vee- ja soojusvarustus, transpordi- ja liiklusvahendid (sõiduautod, veoautod, rongid, lennukid jne).

- Tootmisvahendid
Tootmisvahendite alla koondatakse kõik ressursid, mida ei ole teistes kategooriates mainitud, näiteks tooraine või tootmismaterjalid, kontorimaterjalid ja kontorisisustus.

Ressursid			Rakendused								Riistvara					Infrastruktuur					...
			Meil	Andmebaasi server	Office'i rakendused	SAP	EDI	AutoCAD	Kalender		Internetiühendus	Kohtvõrk (LAN)	Failiserver 1	Failiserver 2		Töökoht	Ladu		Telefoniühendus	Faks	
Äriprotsess		WAZ	4	92	24						48										
	WAZ	kWAZ	4	18	24						48										
Protsess GP1	92	72	1	1	4	1	3	-	4		**J**	1	1	-		1	-		1	-	
Protsess GP4	168	48	**J**	-	1	-	-	-	**J**		-	1	-	1		-	1		-	2	
Protsess GP5	24	24	-	1	1	-	-	1	-		-	1	1	-		-	-		-	-	

Tabel 8. Näide ressursside tuvastamisest koos kasutusmäära ja taaskäivitusaja kohta käivate andmetega

Kriitilise protsessi jaoks vajalike ressursside esitamisel tuleks hinnata ja dokumenteerida ka vastavat kasutusmäära. See näitab kaudselt, kuidas selle ressursi katkemine protsessi jätkumisele mõjuks. Mida kõrgem on kasutusmäär, seda suuremad on tagajärjed ressursi kadumisel. Kasutusteguri määramisel on ennast kõige paremini tõestanud 3-5-astmeline skaala. Võimalikud kasutusmäärad, toetudes protsessidevahelisele sõltuvusmäärale, oleksid näiteks 1=väga kõrge (protsessi jaoks asendamatu), 2=kõrge (protsessi jaoks oluline), 3=keskmine (vajalik) ja 4=madal (vaata tabel 8).

Hiljem tuleb selle sammu läbiviimisel tuvastada ka *Single points of Failure* ehk väga kriitilised ressursid,. mille rivist väljalangemine põhjustaks (osa) protsessi täieliku katkemise. Need ülimalt kriitilised protsessid tuleb dokumenteerida ning võimalikult kiiresti tuleb luua meetmed nende protsesside kindlustamiseks.

Tavarežiimi ressursside esitamise kõrval tuleb kindlaks teha ka nõuded hädaolukorrarežiimi ressurssidele. Seejuures tuleb jälgida, et

- igas äriprotsessis ei lubata hädaolukorrarežiimi,
- hädaolukorrarežiimi korral võib üle minna alternatiivsetele protsessidele (näiteks IT-lahendustelt üleminek paberkandjale või käsitsitöötlemisele)
- hädaolukorrarežiim seisneb selles, et protsess toimub vähendatud jõudlusega, väiksemate nõuetega ressursile, aga ka väiksema sisendi ja väljundiga.

Iga kriitilise protsessi juures tuleb dokumenteerida, kuidas hädaolukorrarežiim välja näeb ja milliseid ressursse selleks vajatakse. Kui taaskäivitamine toimub mitmes astmes, tuleb iga astme jaoks määrata vajalikud ressursid (vt tabel 9).

Protsess D	Tavarežiim	Hädaolukorrarežiim			
Ressursid		≤ 2 tundi	≤ 24 tundi	≤ 48 tundi	≥ 48 tundi
Töökoht	8	2	2	4	8
Rakendus H	8	2	2	4	8
Rakendus B	4		1	2	4
Telefoniühendus	8	1	2	2	8
Ekspert	8	2	2	4	8

Tabel 9. Näide ressursside tuvastamise kohta tava- ja hädaolukorrarežiimi korral

Kuna kõik ressursid ei ole niivõrd nähtavad nagu töökohaarvuti või intranet ning mõningaid käitusvahendeid märgatakse alles siis, kui neid ei ole enam võimalik kasutada, nõuab vajalike ressursside väljaselgitamine hoolikust ja vilumust.

Ressursse võib koguda koos kahjude analüüsiga või pärast prioriteetide kindlaksmääramist. Esimese variandi eeliseks on see, et spetsialiste ei ole vaja teist korda küsitleda ja neilt ei ole vaja uuesti andmeid koguda. Teise variandi eeliseks on see, et ressursside kogumine piirdub ainult kriitiliste äriprotsessidega ja on seega vähem mahukas.

5.1.2.8 Ressursside kriitilisus ja taaskäivitusajad

Kriitilisus ja nõuded ressursside taaskäivitamisele tulenevad reeglina protsesside kriitilisusest ja nõuetest taaskäivitusele, mille käigus neid ressursse kasutatakse. Kriitilisuse edasikandumisel tuleb arvestada sellega, kas ressurssi kasutatakse mitmes protsessis ja milline on üksikute protsesside ressursi kasutustase (vt tabel 8). Seetõttu kehtivad siinkohal samad põhimõtted nagu kaitsevajaduse edasikandumise korral BSI standardi 100-2 järgi: maksimumipõhimõte, kumulatsiooniefekt ja jaotusefekt. Üksikute ressursside kriitilisust (nt e-post) võib tõsta olenemata äriprotsessist tulenevatest nõuetest, tehes seda juhtkonna otsusega. Ressursside taaskäivitumisaegade määramisel tuleb arvestada mõningate raamtingimustega:

- Kui ressursi kasutamine on hädaolukorrarežiimis vajalik, sõltub selle taaskäivitusaeg hädaolukorrarežiimile määratud taaskäivitusajast. Kui seda hädaolukorrarežiimis ei vajata, sõltub see tavarežiimi hiliseimast taaskäivitusajast.
- Osaliselt on võimalik protsessiks vajalikud ressursid paralleelselt taastada, aga mõningad ressursid vajavad kindlat järjekorda. Näiteks saab andmeid alles siis sisestada, kui vastav rakendus (nt andmebaas) on installeeritud. Rakendused saab aga taastada alles siis, kui on olemas IT-süsteem, mis omakorda on võimalik alles luua siis, kui infrastruktuur (infrastruktuur-WAZ + IT-WAZ + rakenduse-WAZ koos andmetaastega < protsessi taaskäivitamine) on taastatud. Sellest tulenevalt on ressursside taaskäivitusajad tihtipeale lühemad kui protsesside omad. Samas sõltub see hädaolukorrarežiimi tüübist (milliseid

ressursse hädaolukorrarežiimiks kasutatakse) ning astmelise taaskäivituse korral erinevate astmete kasutustasemest (millal kui palju ressursse vajatakse).

Lisaks peaks koos ressursside eest vastutava isikuga välja selgitama, kuivõrd peab ressursside korral arvestama seadistus- ja käivitusaegadega, mis viivad maksimaalselt lühikeste käivitusaegadeni, või kuivõrd peab arvestama erinevate ressursside vaheliste sõltuvustega.

Nõuded ressursside taaskäivitumisele määrab tihtipeale äriprotsesside eest vastutav isik. Lisaks võib tulemuste hindamiseks kasutada ka *Bottom-Up*-lähenemist. Praktika on näidanud, et on soovitatav küsitleda kriitiliste alade ressursside eest vastutavaid või neid kasutavaid isikuid, et teada saada, millised ressursid on nende arvates kriitilised ja kuidas üksikute ressursside rivist väljalangemist märgatakse. Kuna protsesside eest vastutavatel isikutel on idealiseeritud ja ainult enda äriprotsessile suunatud nägemus, võib lihttööliste igapäevase tegelikkuse nägemisest olla täiendav abi ja kontroll.

5.1.3 BIA aruanne

Tööprotsesside mõjuanalüüsi aruanne peaks sisaldama põhilist teavet, mis antud analüüsi jooksul koguti, ning lisaks peaks aruanne sisaldama ka põhjendusi. Tööprotsesside mõjuanalüüsi aruanne peaks sisaldama vähemalt järgmiseid punkte.

- Ülevaade juhtimisest
- Tööprotsesside mõjuanalüüsi tegutsemismudel (näiteks viide BSI standardile 100-4)
- Protsessikaart: protsess, sõltuvus, protsessijada ja nende panus ärisihtide saavutamiseks
- Vaadeldud organisatsiooniüksused ja vajadusel ka väljajäetud äriprotsessid
- Kriitilisuse hindamisel arvesse võetud raamtingimused, kasutatud meetodid ja tegutsemisviisid
- Kahjuanalüüsi raamtingimused
- Protsesside üksikanalüüs
- Nimekiri kriitilistest protsessidest, mille esmaseks prioriteediks on taaskäivitamine
- Kriitiliste äriprotsesside ja taaskäivitamiseks vajalike ressursside nõuete ülevaade.

Aruande koostamise eest vastutab hädaolukorra spetsialist. Aruanne peaks saama kõigi organisatsiooniüksuste juhtide käest kirjaliku kasutusloa ning minema siis juhatusele kinnitamiseks.

5.2 Riskianalüüs

Riskianalüüsi kasutatakse kriisihalduse kontekstis selleks, et tuvastada ohtusid, mis võivad põhjustada äriprotsesside katkemise, ja hinnata sellega seotud riske. Eesmärkideks on

- olemasolevad riskid otsustajatele nähtavaks teha,
- vajadusel töötada välja strateegiad ja vastumeetmed, et neid riske juba varem vähendada ja institutsioonide robustsust tugevdada ning
- määratleda stsenaariumid, mis individuaalsete kriisiplaanide jaoks luua tuleb.

Riskianalüüsi läbiviimine on kriisihalduses valikuline, kuna parimal juhul on riski- või informatsiooniturbehaldus riskiennetuse eesmärgi juba saavutanud. Kui riskianalüüsi, mis hõlmaks kriisihalduse kehtivusalasid ja kõiki vaadeldavaid ressursse, ei ole mitte üheski teises institutsiooni haldusüksuses läbi viidud, siis tuleb kriisihalduse raames vastav riskianalüüs läbi viia. Eriline tähelepanu on siinkohal pööratud kriitilistele äriprotsessidele ja ressurssidele.

Riskianalüüsi klassikaliseks lähenemisviisiks on esmalt institutsiooni, protsessi või ressurssi puudutava ohu määratlemine ja riskihinnangu läbiviimine. Riske liigitatakse lähtuvalt kahju mõjust, mis juhtumi korral tekkida võib, ning lähtuvalt kahju tekkimise tõenäosusest. Riskianalüüsi läbiviimisel peaks arvestama järgmiste aspektidega.

- Kõiki riske ei ole võimalik määratleda. Alati on mõni risk, millega ei ole arvestatud. Riskianalüüsi läbiviimisel ei tohiks üritada tuvastada kõiki riske, mis kunagi relevantseks muutuda võiksid, vaid tuleb leida mõistlik kompromiss.

- Juhtumise tõenäosust saab ainult subjektiivselt oletada. Ainult väheste riskide, eelkõige operatsiooniriskide, vallas on olemas läbimõeldud ja konkreetsed arvud. Kuna raamtingimused võivad väga kiiresti muutuda, on veel üheks probleemiks tõsiasi, et minevikusündmustele tuginedes ei ole võimalik teha järeldusi tuleviku tarbeks.

5.2.1 Riski tuvastamine

Riskianalüüsi esimeseks sammuks on kriitiliste äriprotsesside ohufaktorite ja riskide määratlemine. Ohufaktorite all mõeldakse ohte, mis võivad turvaaukude kaudu konkreetselt protsessidele ja ressurssidele mõjuda.

Erinevalt „ohustamisest" hõlmab „riski" mõiste juba hinnangut ning näitab sellega, et ohust võib institutsioonile tekkida kahju.

Kui tööprotsesside mõjuanalüüsi korral vastati küsimusele, millised on protsessi katkestuse tagajärjed institutsioonile, siis nüüd on küsimuseks, et mis olid katkestuse võimalikud põhjused. Seejuures uuritakse nii riske protsessitasandil kui ka riske ressursside tasandil. Protsessitasandi riskiks võib olla näiteks ühe või mitme (kriitilise) ressurssi rivist väljalangemine. Riskianalüüs ressursitasandil otsib seejärel nende kriitiliste ressursside rivist väljalangemise põhjust.

Riske on võimalik kategoriseerida erinevate, üksteisest sõltumatute tunnuste abil:

- sisesed/välised riskid,

- otsesed/kaudsed riskid,

- institutsiooni poolt mõjutatavad/mitte mõjutatavad riskid

Riskide identifitseerimisel on oluline struktureeritud ja süstematiseeritud tegutsemine, mille käigus arvestatakse erinevate riskitüüpidega. Siinjuures võib kasutada tuntud meetodeid nagu kogumismeetod või otsingumeetodid. Kogumismeetodite hulka kuuluvad näiteks kontrollnimekirjad, SWOT-analüüs (tugevused, nõrkused, võimalused ja ohud) või interviud. Kogumismeetodid sobivad eriti hästi ilmselgete riskide tuvastamiseks. Otsingumeetodeid kasutatakse seevastu tulevaste või vähem ilmselgete riskide identifitseerimiseks. Siia hulka kuuluvad vea- ja mõjuanalüüs, HAZOP (*Hazard and Operability Study*), veapuu analüüs (*Fault tree analysis* – FTA), morfoloogilised ja staatilised meetodid, aga ka ajurünnak, võimalikult paljude ideede genereerimine või Delphi-meetod. Kuna kõigil meetoditel on oma plussid ja miinused, siis tuleks võimalusel kasutada mitut üksteist täiendavat meetodit.

Riskiidentifitseerimise baasiks on hea kasutada infosüsteemide etalonturbe ohukatalooge [BSIGK]. Nendes on ohuklasside jaoks suur ohtude valik.

- Vääramatu jõud,

- organisatsioonilised

- puudused, inimvead,

- tehnilised rikked ja

ründed.

Informatsiooniriskide identifitseerimiseks ressursitasandil sobib kasutada „Riskianalüüsi infosüsteemide etalonturbe põhjal", lähtuvalt BSI standardist 100-3 [BSI3]. Kui infosüsteemide etalonturbe järgi on välja töötatud turvakontsept, siis on võimalik suur osa vajalikust informatsioonist antud struktuurianalüüsist üle võtta. Riskianalüüsis lisaks vaadeldud ressursside puhul, millel pole tulemusi üheski informatsiooniturbe halduses, tuleks viia läbi täiendav riskianalüüs.

5.2.2 Riskide hindamine

Järgmise sammuna tuleb hinnata tuvastatud riskide tähtsust. Selleks võib teha oletusi nii tekketõenäosuse kui ka oodatavate kahjustuste suhtes. Selline toimimisviis toob endaga kaasa tuntud probleemid. Üldjuhul on kindlad andmed tekkevõimalikkuse kohta olemas ainult kindlate valdkondade kohta, näiteks looduskatastroofid. Seepärast tuleb tekketõenäosuse hindamiseks kasutada kvalitatiivset lähenemist. Näitlikustava materjalina näidatakse tabelis

10 riskide tekketõenäosuse kategoriseerimist ning nende omavahelist piiritlemist. Nii astmete arv kui ka kriteeriumid tuleb igal institutsioonil individuaalselt määratleda.

Ebatõenäoline	Võimalik	Tõenäoline	Väga tõenäoline
Iga 10 aasta tagant või harvem	Umbes kord aastas	Umbes kord kuus	Kord nädalas või sagedamini

Tabel 10. Näide tõenäosusastmete kohta

Äriprotsessi katkestuse korral oodatavate kahjude hindamine on tööprotsesside mõjuanalüüsis kajastatud kas kvalitatiivses või kvantitatiivses vormis. Kvantitatiivse lähenemise korral tuleb arvestada, et sellisel moel saadud arvud on umbkaudsed ja ainult vähesel määral usaldatavad. Võimaliku kahju suuruse hindamisel on soovitatav seega kasutada kvalitatiivset lähenemismeetodit.

Riski hindamiseks vastandatakse omavahel tekke võimalikkus ja võimalik kahjude suurus. Neid, nagu ka eelnevaid hinnanguid, liigitatakse vastavalt väärtusele neljaks: „madal", „tavaline", „kõrge" ja „väga kõrge". Üks võimalus riskide kategoriseerimiseks on ära toodud järgmises tabelis: „madal", „keskmine", „kõrge", „väga kõrge". See tuleb aga iga institutsiooni jaoks eraldi kindlaks määrata

		Mõju / Kahju			
Tõenäosus		**Madal**	**Normaalne**	**Kõrge**	**Väga kõrge**
	Väga tõenäoline	madal	keskmine	kõrge	,väga kõrge
	Tõenäoline	madal	keskmine	kõrge	kõrge
	Võimalik	madal	madal	keskmine	keskmine
	Ebatõenäoline	madal	madal	madal	madal

Tabel 11, Näide riskikvalifikatsiooni kohta

Riske võib tuvastada ja näidata erineval moel. Siinkohal võib abi olla abiprogrammide kasutamisest. Järgmises tabelis näidatakse riskide võimalikku tuvastamist.

Põhjus	**Risk**	Stsenaarium	**Mõju**	**Tõenäosus**	**Riskihinnang**	**Nõrgad kohad**	**Strateegia**	**Meetmed**	**Vastutav**
Kaablipõleng Lühis soojenemine	Tulekahju	Katkestus andmekeskus	Väga kõrge	Võimalik	Keskmine	Ruumi jagamine tuletõkke .. vahel			
Välise vooluvarustuse katkemine, sisemise vooluinfrastruktuuri katkestus	Voolukatkestus	Katkestus andmekeskus	Kõrge	Võimalik	Keskmine	Kütuse kogus piisav ainult viieks tunniks, ainult 50% serveritest on hädaolukorravooluvarustusega ühenduses		Täiendavad voolugeneraatorid	

Tabel 12. Näide riskituvastuse kohta

Riskidest ülevaatliku pildi andmiseks kasutatakse tihtipeale riskimaatriksit, mis võib aidata vastava riskistrateegia valimisel.

5.2.3 Grupeerimine ja stsenaariumite koostamine

Edasistes sammudes, millega tuvastatud riskid paremini kasutatavaks muudetakse, tuleks need konsolideerida.

Konkreetsete ettevaatusabinõude tuvastamiseks tuleb suur hulk riske mugavalt kasutatavaks teha. Kui riske uuritakse protsessitasandil, võib olla mõttekas paigutada iga vaadeldud äriprotsessi jaoks olulised riskid vastavale protsessile määratud gruppi. Ressursitasandil saab ressursi jaoks oluliste riskide hulka vähendada sarnaste riskide konsolideerimise kaudu.

Kuna ei ole võimalik luua iga riski jaoks eraldi kriisiplaani, tuleks välja töötada stsenaariumid, mille alla oleks võimalik riske liigitada. Et hoida kriisiplaanide arv võimalikult ülevaatlik, tuleks välja töötada võimalikult praktikalähedased ja üldised kriisistsenaariumid. Kriisistsenaariumid lähtuvad seejuures riskide mõjust äriprotsessidele. Arendamisel on abiks stsenaariumitehnika, millega uuritakse sündmuste erinevat ajalist arengut ja eskalatsioonivõimalusi (ülimalt positiivsetest kuni ülimalt negatiivseteni). Seeläbi on võimalik tuvastada vastava hädaolukorra stsenaariumiga seotud riske. Kui valitakse stsenaariume spetsiifiliste hädaolukorraplaanide väljatöötamiseks, tuleb jälgida, et kasutataks neid hädaolukorra stsenaariume, mis põhjustavad kõige suuremat kahju ning mille teke on institutsiooni jaoks kõige tõenäolisem. Praktika on näidanud, et kõige parem on kasutada 5-15 stsenaariumi. Üldised kriisistsenaariumid on näiteks järgmised.

- Töökoha (osaline) rivist väljalangemine (näiteks üleujutus, põleng, piirkonna sulgemine, ligipääsukontrolli katkestus)
- Kommunikatsiooniinfrastruktuuri või informatsioonitehnika katkestus,
- süsteemide või rajatise laialdane katkestus (näiteks tootmises)
- Kriitilise hulga töötajate rivist väljalangemine (näiteks pandeemia, toiduainemürgitus, streik)
- Teenusepakkujate rivist väljalangemine (näiteks tarnijad, voolutarnija)

Kriisistsenaariumeid võib välja töötada ka enne tööprotsesside mõjuanalüüsi läbiviimist või sellega samal ajal. Kuigi äriprotsessi katkestuse korral ei mängi põhjus mingit rolli, võib see mõningatel vastutavatel isikutel aidata endale konkreetseid stsenaariume ette kujutada ning teha nendest omakorda järeldusi võimalike tagajärgede kohta.

5.2.4 Riskistrateegiavalikute tuvastamine

Riske on võimalik aktsepteerida, edastada, vältida või vähendada. Strateegiavalikud on suunavad otsused, mis on otseselt riskide käsitlemisega seotud [BSI3]. Iga kriitilise äriprotsessi ja iga riski kohta dokumenteeritakse ja määratakse sobiv strateegia. Sellele järgnev riskistrateegia valik paneb aluse hilisemale jätkustrateegia valimisele. Pärast riskistrateegia teostamist jääv jääkrisk aitab otsustada, millistele äriprotsessidele tuleb individuaalsed hädaolukorraplaanid luua.

Riskistrateegia valimisel ei arvestata mitte ainult riskisituatsiooniga, vaid muuhulgas ka majanduslike, tegevusega seotud ja tehniliste aspektidega. Allpool on võimalikke riskistrateegiaid lähemalt kirjeldatud.

Riski ülevõtmine

Riski ülevõtmisel aktsepteeritakse tuvastatud risk. Seda valikut kasutatakse tavaliselt siis, kui tuvastatakse väikese tõenäosuse ja madala kahjupotentsiaaliga katkestusstsenaariumid. Muud põhjused sellise otsuse tegemiseks võiksid olla näiteks see, et aluseks oleva ohu vastu ei ole teada ühtegi tõhusat lahendust, või tõhusa lahenduse maksumus ületab kaitstava väärtuse.

Riski ülekandmine

Riski ülekandmisel kantakse risk üle mõnele teisele institutsioonile. Seda võib teha kas kindlustuslepingu sõlmimise või alltöövõtjate kaudu. Kindlustuslepingu sõlmimisega on võimalik otseseid rahalisi kahjusid vähendada, sest tekkiv kahju korvatakse kas osaliselt või isegi täielikult (näiteks tulekahju, veekahjustus või vargus). Reeglina ei korvata aga kõrvalkulusid, mis on otseselt või kaudselt tekkinud äriprotsesside katkestuse tõttu. Eelkõige

käib see mainekahju kohta. Lepingu sõlmimisel tuleks arvesse võtta erilisi raamtingimusi ja samuti kõiki lepingu erandeid. Arvestada tuleb ka asjaoluga, et enne, kui kindlustus kahju katab, võib juhtuda, et pikem periood tuleb rahaliselt ise katta.

Veel üheks riski ülekande võimaluseks on mõjutatud äriprotsesside (osaline) hankimine alltöövõtuna. Mõttekas on see näiteks siis, kui alltöövõtja on majanduslikel või tehnilistel põhjustel paremini võimeline antud riskiga toime tulema. Siinkohal tuleb jälgida, et osariskid nagu mainekahjustus ja tegevuse piiratus jäävad, tulenevalt sõltuvatest protsessidest, ikkagi institutsioonisiseseks. Lisaks tekkivad uued riskid, mis tulenevad sõltuvusest teenusepakkujast.

Riski vältimine

Kui mõnel äriprotsessil on selle spetsiaalse kulgemise tõttu kõrge kriitilisus, võib sobivaks strateegiaks olla protsessijada või keskkonnatingimuste selline muutmine, et vastav oht kaotab oma olulisuse. Kui äriprotsess ei ole, tulenevalt tuvastatud riskist, ettevõttele enam vastuvõetav, võib isegi olla vajalik protsess seisata ja asendada see täiesti uue protsessiga. Riski vähendamine tähendab alati, et vaadeldud riski tõenäosus või kahju ulatus on vähendatud nullini.

Riski vähendamine

Enimvalitud strateegiaks on riski vähendamine. Selle korral vähendatakse riski tõenäosust või kahju suurust. Seda on võimalik teha nii meetmete rakendamise kui ka protsessijada muutmise kaudu.

Riskid koonduvad hulgaliselt ühte kindlasse punkti näiteks siis, kui kõik äriprotsessid luuakse ühes andmekeskuses. Sellist meetodit kasutatakse tänapäeval paljudes institutsioonides. Sellisel viisil kulude kokkuhoidmisele tuleb aga vastandada suuremat riski. Riskivähenduse meetmeks võiks olla näiteks äriprotsesside ja seega ka riskide jaotamine mitmesse andmekeskusesse.

5.2.5 Riskianalüüsi aruanne

Riskianalüüsi aruanne ei peaks dokumenteerima mitte ainult tulemusi, vaid ka kasutatud meetodit. Sellest tulenevalt saame võimalikuks struktuuriks:

- ülevaade juhtimisest,
- riskianalüüsis kasutatud meetodid,
- nimekiri riskidest ning nende võimalik grupeerimine,
- riskihinnangu tulemused,
- riskistrateegia valikud kriitiliste protsesside tarvis,
- riskistrateegia väljavalimine.

Riskianalüüsi aruande koostamise eest vastutab hädaolukorra spetsialist. Aruanne tuleb esitada juhatusele, kes peab selle ka kinnitama.

5.3 Hetkeolukorra fikseerimine

Tööprotsesside mõjuanalüüsiga tuvastati kriitilised protsessid ja nende (kriitilised) ressursid. Selleks, et ühest küljest oleks võimalik umbkaudu hinnata erinevateks strateegiateks vajalikku tegevusraamistikku ja sellega seotud investeerimiskulutusi ja teisest küljest tuvastada analüüsi (milline peaks hetkeolukord tegelikult olema) kaudu veel realiseerimist vajavad meetmed, on järgmises sammus väljatöötatava jätkustrateegia valiku ja strateegiavaliku tegemiseks vaja välja selgitada hädaolukorraks valmisoleku meetmete ja hetkel võimalike taaskäivitusaegade hetkeolukord.

Hetkeolukorra analüüs võib piirduda põhiliste ressurssidega (näiteks kriitilised äriprotsessid). Mõningane informatsioon on võimalik üle võtta turbekontseptsiooni struktuurianalüüsist BSI standardi 100-2 järgi. Lisada tuleb informatsiooniturbe juhtimises vaatluseta jäänud ressursid.

5.4 Jätkustrateegia

Äritegevust saab jätkata, täpsemalt taaskäivitada, erineval moel. Strateegiavalikud erinevad selliste parameetrite poolest nagu taaskäivitusaeg, kulud ja lahenduse usaldusväärsus. Eesmärgiks on alternatiivide tuvastamine ja institutsiooni jaoks parima lähenemise väljavalimine. Selleks kantakse kriisihalduse suunistes määratletud kriisihalduse algatamise raames väljatöötatud suunav üleinstitutsiooniline hädaolukorrastrateegia *Top down*-meetodi abil koos täpsustustega üle protsessi- ja ressursitasandile.

5.4.1 Jätkustrateegiate väljatöötamine

Jätkustrateegia alternatiivid pakuvad mitmeid võimalusi, kuidas täita lünk hädaolukorraks valmisoleku meetmete hetke- ja vajaliku olukorra vahel. Meetmed peavad täitma järgmiseid raamtingimusi.

- Protsesside ja
- ressursside jaoks kindlaks määratud taaskäivitusaegadest ja reguleeriva loomuga nõuetest tuleb kinni pidada.
- Alternatiivide kulud peaksid olema vastuvõetavas vahekorras kindla ajaperioodi vältel oodatava kahjuga, st nad peaksid olema majanduslikult mõttekad.

Tulenevalt institutsiooni eesmärkidest, nagu ka selle põhilisest tegevusalast, on kriisihalduse suunistes kirjeldatud üleinstitutsiooniliselt määratud hädaolukorra strateegiat. See moodustab raamistiku edasiseks tegevuseks. Institutsioonitasandil määratakse seejärel kindlaks jätkustrateegia valikud ja üleüldised põhimõtted. Ühte näidet näete järgmises tabelis.

Valik	Kirjeldus	Riskivaatlus
Minimaalse tõhususega lahendus	Kindlustatakse ainult kõige kriitilisemad protsessid Meetmete kogumaksumust tuleb piirata ... le Kahjupotentsiaali tuvastatakse enamjaolt kindlustuse kaudu.	Kõrge jääkrisk
Madala tõhususega lahendus	Kindlustatakse ainult kõrge prioriteediga protsessid. Meetmete kogumaksumust tuleb piirata	Keskmine kuni kõrge jääkrisk
Keskmise tõhususega lahendus	Kindlustatakse põhilised tuumprotsessid. Meetmete puhul tuleb jälgida, et enamjaolt kasutataks institutsioonisiseseid võimalusi.	Keskmine jääkrisk
Kõrge tõhususega lahendus	Kriitilised äriprotsessid kindlustatakse laiaulatuslikult. Kõrge prioriteet tuleb omistada seadustest ja lepingutest kinnipidamisele ning mainekahjustuste ärahoidmisele.	Madal jääkrisk

Tabel 13. Näide üleinstitutsiooniliste valikute kohta

Pärast üleinstitutsioonilise jätkustrateegia kindlaksmääramist tuleb see protsessi- ja ressursitasandile tuua. (Kriitiliste) äriprotsesside ja ressursside tarvis on vaja erinevaid tegutsemisvõimalusi konkretiseerida. Allolevas tabelis tuuakse puudulik näide protsessitasandi valikutest. Põhjalikud kirjeldused, võimalikud tegevusalternatiivid ja lisanäiteid kõigi meetmete kohta leiab lisast A.

	Protsess „andmekeskus”	**Protsess „juhatuse töökoht”**
Minimaalse tõhususega lahendus	Teenindusleping hädaolukorrarežiimiks	Sisene lahendus: vähemkriitiliste töökohtade vabastamine kriitiliste tarvis ja kodutöökohad kõrgeima prioriteediga töökohtade tarvis.
Madala tõhususega lahendus	„Cold standby” varuandmekeskus	Lahendus koostööd tegevate partnerlussidemete kaudu.
Keskmise tõhususega lahendus	„Warm standby” varuandmeksekus	Teenindusleping „sissekolimiseks valmis büroohoone”
Kõrge tõhususega lahendus	„Hot standby” varuandmekeskus	Teine büroohoone

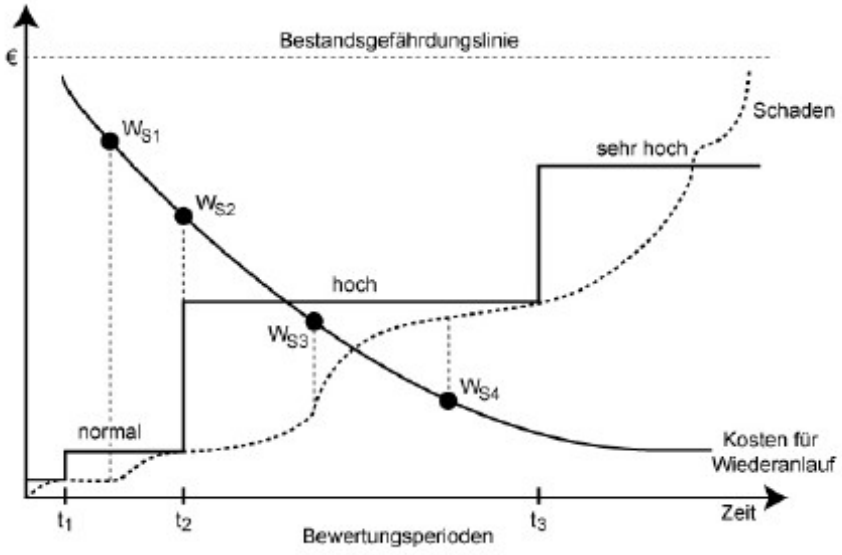
Tabel 14. Näide protsessivalikute kohta

5.4.2 Tasuvusanalüüs

Kriisihalduse üks põhilisi eesmärke on äritegevuse jätkamise piisav kindlustamine võimalikult vastuvõetavate kulutustega. Hea jätkustrateegia valimisel võib abiks olla erinevate variantide kulude-tulude analüüs. Selleks tuleb omavahel vastandada jätkustrateegia meetmete kulutused ning nende kasutegur. Lugematud materiaalsed ja mittemateriaalsed mõjutegurid (vt ka peatükk 5.4.3) võivad valiku tasuvust kas suurendada või vähendada. Kuna ei ole võimalik arvestada kõiki mõjufaktoreid, tuleks jätkustrateegia tasuvusanalüüs viia läbi pragmaatilise lähenemise kaudu. Abiks võiksid olla järgmised näited.

Samm 1. Hädaolukorra tõttu tekkinud protsessikahju väljaselgitamine

Protsessi katkestuse kahjupotentsiaal määrati ära juba tööprotsesside mõjuanalüüsis, kusjuures kahju ei koosne mitte ainult rahalisest kahjust, vaid, nagu tööprotsesside mõjuanalüüsis kirjeldatud, kujutab kahju endast kõiki negatiivseid tagajärgi, mis institutsioonile tekivad. Jätkustrateegia kasutamist võib vaadelda võimena hoida institutsiooni kahjusid võimalikult kiire taaskäivituse või protsesside alalhoidmise kaudu madalatena. Strateegilise valiku kasu on seda suurem, mida väiksem on taaskäivitumiseni või taastamiseni tekkiv kahju. Joonisel 8 näidatakse kahju võimalikku kulgu (katkendlik joon) ja tööprotsesside mõjuanalüüsi üldise kahju kulgu, aga ka erinevate strateegiate taaskäivitusaegu W_{Si}.



Joonis 8. Kahjukulg ning kulutused taaskäivitamiseks

(Bewerungsperioden – hinnanguperioodid, Zeit – aeg; normal – tavaline; hoch – kõrge; sehr hoch – väga kõrge; Bestandsgefärdungslinie – eksistentsi ohustav piir, Kosten für Wiederanlauf - Kulud taaskäivitamiseks Schaden - Kahju)

Samm 2. Jätkustrateegia kulude väljaselgitamine

Teise sammuna selgitatakse välja üksikute strateegiliste valikute kulud. Kulud ja jätkustrateegiad tuleks institutsioonis tuvastada ja neid tuleks hinnata tunnustatud finantsplaneerimise meetodite järgi. Siia hulka kuuluvad peale soetamiskulude ka jooksvad kulud regulaarsete hoolduste, koolituste ja üüri eest ning võimalik, et ka lepingukulud (näiteks varutöökohtade hoidmine mõne välise teenusepakkuja juures). Olulist rolli mängib siinkohal hädaolukorra meetmete hetkeolukord ja täitmist vajavad lüngad, mis tuleb üksikute strateegiliste valikute suhtes välja selgitada. Selleks tuleb võrrelda hetkeolukorda ja olukorda, mis tegelikult valitsema peaks.

Samm 3. Tasuvusanalüüsi lõpuleviimine

Seejärel liidetakse kahe eelmise sammu tulemused kokku otsustusabiks. See otsustusabi peaks näitama, milliseid kulutusi on tarvis teha, et saada teatud tulemus. Reeglina tähendavad lühemad taaskäivitusajad väiksemaid kahjustusi, aga ka suuremaid investeeringuid, kuid piiravate raamtingimustega strateegilised valikud võivad seda reeglit eirata. Järgmised näited näitlikustavad fiktiivsete arvudega otsustusabi ülesehitust. Need ei

hõlma kõiki võimalusi andmekeskuse või töökohtade kindlustamiseks ega ole ka täielikult määratletud. Andmekeskuse alternatiivsete turbevõimaluste üksikasjaliku kirjelduse leiate lisast A.

Protsess „andmekeskuse käitus” MTA =10 päeva	**Taaskäivitus -aeg**	**Kulud**	**Kahju kuni taaskäivitus eni**	**Usaldusväärsus/ra amtingimused/piir angud**
S1. Ooterežiim (*standby*) andmekeskus / „Hot”-lahendus: täiuslik, üleliigne IT-	< 6 tundi	5 mil. eurot	madal	väga kõrge
S2. Vahepealne lahendus: andmekeskus; kogu IT olemas; hädaolukorras vajalike varundatud andmete installeerimine	6-24 tundi.	3 mil. eurot	madal kuni keskmine	kõrge
S3. Minimaalne lahendus: hädaolukorras vajaliku riistvara hankimine ja tarkvara	2-10 päeva	1-1,2 mil. eurot	keskmise lt kõrge	Jääkrisk: riistvara hankimine; maksimaalne taaskäivitusaeg 10 päeva

Protsess „andmekeskuse käitus” MTA =10 päeva	**Taaskäivitus -aeg**	**Kulud**	**Kahju kuni taas-käivituseni**	**Usaldusväärsus/ raamtingimused/ piirangud**
rakenduste ning MTA varunduskoopia				seega puudub ka jääkpuhver
S4. Teenindusleping „Hädaabi andmekeskus” teenusepakkujaga A	2 päeva	700 000 eurot	keskmin e	Jääkrisk: hädaolukorras teenusepakkujalt
		1,3 mil. eurot	keskmin e	Kõrgendatud prioriteediga lepingu sõlmimine
S5. Teenindusleping „Hädaabi andmekeskus” teenusepakkujaga B	2 päeva	500 000 eurot	keskmin e	Jääkrisk: hädaolukorras teenusepakkujalt saadavad ressursid; jääkrisk: teenusepakkuja usaldusväärsus ja

Tabel 15. Näide 1 otsustusabi tasuvusanalüüsi kohta

Protsess „juhatuse töökoht” MTA =14 päeva	Taaskäivitus -aeg	Kulud	Kahju kuni taaskäivitu seni	Usaldusväärsus/r aamtingimused/piir angud
S1. Üüritud ruumid	2 päeva	2000 eurot/ töökoht	keskmine	
S2. Vajadusel konteinerite muretsemine	7-12 päeva	700 eurot/ töökoht	kõrge	Jääkrisk: paigaldusvõimalus ainult ettevõtte kinnistule ja seega ebasobilik lahendus juhuks, kui ettevõtte kinnistule ei ole
S3. Töökoht kodus	12 tundi	200 eurot/ töökoht	madal	Hetkel sobib maksimaalselt 10% töökohtadest. Jääkrisk: internetiühenduse ja võrgupunkti kättesaadavus, arvuti ja dokumendid paiknevad büroos ja mitte kodusel töökohal.

Tabel 16. Näide 2 otsustusabi tasuvusanalüüsi kohta

Tähelepanu! Näites toodud taaskäivitusajad ning kulud on fiktiivsed ja näitlikustavad. Töökohtade kujundamisel peab iga institutsioon konkreetsetest kasutusjuhtudest ja vajadustest lähtuvalt sobivad väärtused välja selgitama või neid ligilähedaselt hindama!

5.4.3 Jätkustrateegia valik ja konsolideerimine

Tasuvusanalüüsi eesmärgiks on aidata leida sobiv jätkustrateegia. Jätkustrateegia kulud ja seeläbi ärahoitud võimalikud kahjud ei tohiks aga väliste faktorite ja institutsioonisiseste sõltuvuste tõttu jääda ainsaks kriteeriumiks, mida otsustamisel kasutatakse. Raamtingimused, piirangud ja kättesaadavushinnangud tuleks alati otsuse tegemisse kaasata.

Sisemise sõltuvuse saab tuvastada institutsioonisiseste arutelude kaudu. Sisemise lahenduse kasutamine jätkustrateegiana nõuab detailset analüüsi. Põhjalik „peaks olema/on”-analüüs peaks sisaldama vähemalt järgmiseid punkte.

- Kas vajalikest taaskäivitusaegadest peetakse hädaolukorras kinni?
- Kas on sõltuvusi ressursside vahel, mida on üheaegselt vaja mitmes protsessis?

Välised faktorid nagu läheduses asuvate institutsioonide poolt ruumide mitmeotstarbeline kasutamine või eriliste kõrgendatud taaskäivitusnõuetega tähtaegade tähendus erinevatele äriprotsessidele võivad endaga kaasa tuua jätkustrateegia uue hindamise. Välised faktorid tuleks institutsiooni juhtkonnaga läbi arutada ja välja töötada. Näiteks võib mõne näiliselt odava teenusepakkuja halb maine ka institutsioonile üle kanduda, kui hädaolukorraga ei tulda piisavalt toime. Sellest tulenevad kaudsed kulud põhjendaksid siinkohal kulukama lahenduse valikut. Lisaks võivad mõningad jätkustrateegiad pakkuda kriisihaldusest sõltumatut lisaväärtust, näiteks uute laoruumide loomise kaudu.

Niipea kui sisemised sõltuvused ja välised faktorid on tuvastatud, tuleb koostada otsustusnäidis ja see juhtkonnale esitada. Otsustusnäidis võib sisaldada ka soovitusi. Juhatuse ülesandeks on nende arvates parima strateegia kindlaks määramine. Otsus tuleb dokumenteerida ja institutsiooni juhtkonna poolt kirjalikult kinnitada. Kõik ülejäänud kriisihaldusmeetmed peavad lähtuma sellest valitud strateegiast ja neid tuleb hädaolukorraks valmisoleku plaanis täpsustada.

Strateegia väljatöötamine ja strateegia kindlaks määramine on seotud regulaarse täiendusprotsessiga. Kui välistes mõjudes tuvastatakse uusi strateegilisi valikuid või mitmeid muutusi, tuleks koostada uus tasuvusanalüüs või läbi viia konsolideerimisnõupidamine.

5.5 Hädaolukorraks valmisoleku plaan

Hädaolukorraks valmisoleku plaan moodustab jätkustrateegia aluse. See kirjeldab olemasolevaid tingimusi ning sisaldab endas kogu kontseptsiooni väljatöötamise käigus saadud teavet. Hädaolukorraks valmisoleku plaan peaks sisaldama kõiki organisatoorseid ja kontseptuaalseid aspekte, nagu ka kõiki kriisihalduse meetmeid ja tegevusi, mis ei ole otseselt hädaolukorra lahendamisega seotud. Siia hulka kuuluvad

- ennetavad meetmed, mis riskide kahju või tekkevõimalust vähendavad ja institutsiooni vastupidavusvõimet kriisilävendi tõstmisega suurendavad ning ka
- meetmed, mis võimaldavad juhtumi korral kiirest ja mõttekalt reageerida.

Sellest lähtuvalt tuleb hädaolukorraks valmisoleku plaani hoolikalt plaanida, teostada ning regulaarselt täiendada. Hädaolukorraga toimetulekuks vajalik teave, näiteks kontaktinformatsioon või tegutsemisjuhendid, on ära toodud kriiskäsiraamatus (vt peatükk 7.4). Kõik see kokku moodustab hädaolukorraplaani.

5.5.1 Kontseptsiooni peensused, turvalisus ja kontrollid

Jätkustrateegia ennetamise ja realiseerimise ettevaatusabinõud tuleb kindlaks määrata. Peale hädaolukorrarežiimi lahenduste väljatöötamise tuleb tegeleda ka tagasi tavarežiimi pöördumisega ja tööetappidega pärast tavarežiimi taastamist.

Nii detailse kontseptsiooni kui ka hädaolukorra käsiraamatu koostamisel peaksid olulist rolli mängima turvalisuse ja andmekaitse aspektid. Turvalisuse all mõeldakse nii informatsiooniturvet, isikute turvalisust kui ka käituse turvalisust. Kui käsitletavates äriprotsessides töödeldakse salajast teavet, tuleb kaasata ka salajase teabe turbespetsialist. Tuleb kindlustada, et turvalisus oleks kindlustatud nii hädaolukorrarežiimis kui ka üleminekul tavarežiimile, näiteks seaduse poolt etteantud nõuete täitmisel töötajate kaitseks või informatsiooni konfidentsiaalsuse, täiuslikkuse ja kättesaadavuse tagamisel. Sellest lähtuvalt on oluline tihe koostöö turvaspetsialistidega (näiteks infoturbespetsialist, tööturvalisuse spetsialist). Hädaolukorrarežiimi turbekontsepti loomine ei ole kriisihalduse ega kriisispetsialistide algne ülesanne.

Kui see ei ole juba aktuaalse turvaplaani osa, tuleb IT-osakonna infoturbespetsialistil koostada ja realiseerida vastav infoturbeplaan, mis hõlmab kõiki kriisihalduse protsesse, süsteeme ja meetmeid. Infoturbeplaanis vaadeldakse hädaolukorrarežiimiks ettenähtud hädaolukorraprotsesse, taaskäivitusetappe, üleminekuprotsesse ja järeltöid ning kindlustatakse protsesside ja iga vahesammu kohta käiva teabe konfidentsiaalsus ja terviklus. Taastamis- või taaskäivitamisplaani jaoks võib see näiteks tähendada, et kinni tuleb pidada kindlast tööde järjekorrast. Näiteks võib konfidentsiaalseid andmeid taastada alles siis, kui võrgu turvalisus on täielikult taastatud turvalüüsi ja teiste turbemeetmete kaudu tagatud. Kui taaskäivitumise, hädaolukorrarežiimi või üleminekuetapis tuleb seoses infoturbega kompromisse teha, siis tuleb see dokumenteerida, tekkivad riskid tuleb välja tuua ning seejärel tuleb lasta kompromiss juhatuse allkirjaga kinnitada.

Lisaks tuleks detailse kontseptsiooni korral järgida ka institutsiooni siserevisjoni poolt ettenähtud nõudeid. Tuleb välja selgitada, kuivõrd on testid, mida kasutatakse tavarežiimis nõuetekohase käituse kinnipidamise kontrolliks, tööstusspionaaži ärahoidmiseks või väärkasutuse avastamiseks, vajalikud hädaolukorrarežiimis. Soovitatav on teha koostööd siserevisjoniga, et see hädaolukorrarežiimi protsessid üle kontrolliks ja kinnitaks.

5.5.2 Sisu

Hädaolukorraks valmisoleku plaan koostatakse hädaolukorra spetsialisti, hädaolukorra koordinaatorite ja hädaolukorraks valmisoleku meeskonna koostöös. Hädaolukorraks valmisoleku plaani eest vastutab aga lõppkokkuvõttes institutsiooni juhtkond, kes peab selle kinnitama ja kasutusse andma.

Hädaolukorraks valmisoleku kontseptsioon peaks sisaldama vähemalt järgmiseid punkte.

Tegutsemismudel ja realiseerimine

Hädaolukorraks valmisoleku plaaniga antakse ette kindel raamistik, kuidas hädaolukorras äritegevust jätkata, üles ehitada ja kontrollida. Tuleb täpselt kirjeldada, kuidas kriisihalduse erinevad faasid on institutsiooni olemasolevate struktuuridega seotud ning kuidas kriisihalduse tegevust juhitakse ja kontrollitakse. Kriisihaldust tuleb regulaarselt efektiivsuse ja tõhususe suhtes kontrollida. Selleks puhuks on ette nähtud sõltumatu kontrollmeetod.

Tõrke, hädaolukorra ja kriisi definitsioon

Niipea, kui kahjustada saanud alas kuulutatakse välja hädaolukord, asendatakse tavaline äritegevus hädaolukorraga toimetuleku meetmetega. Kõik, mis esimeses paanikas hädaolukorrana paistab, ei pruugi seda olla. On oluline, et iga institutsioon teeks enda jaoks selgeks, mis on tõrge, mis hädaolukord või kriis, ja määraks isiku, kes on volitatud antud otsust tegema.

Ettevaatusabinõud

Kindlaks määratud ettevaatusabinõud, nagu näiteks reatehnika, varuasukohad või hädaolukorras olulised kokkulepped väliste teenusepakkujatega (vt lisa B) tuleb dokumenteerida. Ettevaatusabinõud, mis on kriisihaldusele olulised, kuid on juba infoturbe plaani abil kindlustatud, tuleks üles märkida ning samas tuleks viidata infoturbehalduse või riskihalduse vastavatele dokumentidele.

Seletussõnastik

On oluline, et institutsiooniks loodaks kriisihalduse eesmärkide ja meetmete suhtes ühine mõistmine. Siia kuulub ka ühtlustatud ja selgelt arusaadavate mõistete defineerimine ja dokumenteerimine. Selleks tuleks juba varakult koostada seletussõnastik, mis selgitab kõiki kriisihaldusega seonduvaid mõisteid.

Hädaolukorraks valmisoleku plaani sisu

Hädaolukorraks valmisoleku plaan peaks sisaldama vähemalt järgmiseid punkte.

Üldine

- Dokumentide eest vastutavate isikute kindlaksmääramine
- Dokumendi ja lubamismenetluse klassifitseerimine
- Kehtivusala, versiooni nimetus
- Dokumentide vastuvõtjad ja nende edastamisviisid
- Dokumendistruktuur ja seosed teiste oluliste dokumentidega
- Kasutatud lühendid, seletussõnastik

Organisatsioon ja tegutsemismudel

- Tõrke, hädaolukorra ja kriisi definitsioon
- Vastutuse ülevõtmine juhtkonna tasandi poolt
- Eesmärgid, vastutus, kompetents ja paigutamine teistesse institutsiooni haldussüsteemidesse
- Kriisihalduse integreerimine kõikidesse olulistesse äriprotsessidesse, erialatöösse ja projektidesse
- Hädaolukorraks valmisoleku ja hädaolukorra lahendamise

organiseerimise kirjeldus, täideviimise ja tegevusjärjekorra

kirjeldus.

Äriprotsessi ja kahjude analüüs

- Hädaolukorra stsenaariumid ja mõjud
- Kriitilised äriprotsessid ja nõuded nende kaaskäivitusele
- Prioriteetide nimekiri
- Jätkustrateegiad
- Hädaolukorraks valmisoleku kulud,
- jääkrisk

Organisatoorsed ja tehnilised ettevaatusabinõud

- Üldiste varutöökohtade ja nendele esitatud nõudmiste kindlaksmääramine
- Häiremeetod
- Riski vähendavate meetmete kirjeldus
- Andmete varundamine
- Teatemeetod
- Kokkulepped väliste teenusepakkujatega

Kriisihalduse hilisem lisamine asutuse või ettevõtte struktuuri

- Töötajate informeerimine ja koolitamine
- Hooldus-, test-, ja järelvalveprotsesside integreerimine juba olemasolevatesse sisemistesse protsessidesse

Säilitamine ja kontroll

- Õppuste ja testkäituste kaudu pidev kriisihalduse parandamine,
- hädaolukorraks valmisoleku ja hädaolukorra lahendamise meetmete hooldus ja töötlemine,
- juhtimise kirjeldamine ning kriisihalduse kontroll

Hädaolukorraks valmisoleku plaani koostamise eel tuleks mõelda antud plaani jaotamisele erinevateks mooduliteks. Jagamisel võib vaadelda vastavat sihtgruppi, kes vajab realiseerimiseks üksikuid osi. Samuti võib mõelda, kas oleks mõttekas jagada plaan üldosaks ning põhiosaks. Üldosa sisaldab ainult kriisihalduse üldiseid põhimõtteid ja sobib seega uute klientide ja koostööpartnerite leidmiseks. Põhiosa sisaldab realiseerimiseks vajalikku sisemist ja konfidentsiaalset detailset teavet.

5.5.3 Hädaolukorra valmisoleku plaani tutvustamine ja levitamine

Hädaolukorraks valmisoleku plaani kinnitab juhtkond ja avaldab hädaolukorra spetsialist. Hädaolukorra spetsialist edastab plaani volitatud isikutele. Oluline on, et kõik hädaolukorraks valmisolekuga seotud isikud tunneksid hädaolukorraks valmisoleku plaani sisu ja suudaksid seda igal ajal täita. Tuleb kontrollida, kas on veel isikuid (hädaolukorraga toimetuleku meeskonnast või koostööpartneritest), kes vajavad tööks hädaolukorraks valmisoleku plaani täisversiooni või selle väljavõtteid.

Kuna kriishaldusplaan võib ühest küljest sisaldada konfidentsiaalseid andmeid, teisest küljest aga on see vajalik äriprotsesside kindlustamiseks, tuleb kindlaks määrata, kellele kriishaldusplaan jagatakse ning kuidas seda klassifitseerida. Vastavalt institutsioonile võivad mõlemad punktid olla väga erinevad.

5.5.4 Hädaolukorraks valmisoleku plaani värskendamine

Hädaolukorra spetsialist vastutab selle eest, et hädaolukorraks valmisoleku plaan oleks pidevalt ajakohane ja täiuslik. Hädaolukorraks valmioleku plaani tuleks regulaarselt kontrollida, et see oleks endiselt aktuaalne, ja vajadusel muuta. Samuti tuleks kontrollida, kas on muudetud ärieesmärke või ülesandeid ja sellega koos ka äriprotsesse või tootmismeetodeid või kas muudetud on organisatsiooni struktuuri.

6 Hädaolukorraks valmisoleku plaani rakendamine

Selles peatükis kirjeldatakse, kuidas hädaolukorraks valmisoleku meetmeid plaanida, läbi viia, saata ja kontrollida. Kuna hädaolukorraks valmisoleku meetmete ja turvameetmete vahel on ühilduvusi, tuleks, nagu kontseptsiooni väljatöötamiselgi, koordineerida nende elluviimist infoturbehaldusega.

Meetmete rakendamisel on reeglina kasutada ainult piiratud ressursid (raha, personal). Allpool kirjeldatud sammude eesmärgiks on ettenähtud meetmeid võimalikult tõhusalt rakendada.

6.1 Kulude ja töökoormuse hindamine

Esimene suuremahuline ennetusabinõude kulude hindamine viidi läbi juba jätkustrateegia väljatöötamisel. Pärast kindla strateegia kasuks otsustamist ja selle hädaolukorraks valmisoleku plaanis täpsustamist võib ette võtta oodatavate kulude detailse planeerimise.

Kuna ettevaatusabinõude läbiviimiseks kasutada olevad rahalised vahendid on peaaegu alati piiratud, tuleks iga teostatava meetme puhul määrata, milliseid kulutusi on selleks vaja teha ning kui suur on personalikulu. Siinkohal tuleks eristada ühekordseid ning mitmekordseid kulutusi.

Kui selles faasis selgub, et valitud meetmed ei ole majanduslikult teostatavad, tuleks mõelda vähem kulukate alternatiivmeetodite kasutamisele või kaaluda, kas jääkrisk, mis teostamata meetmete tagajärjel tekib, on institutsioonile vastuvõetav.

Kui hädaolukorraks valmisoleku meetmete realiseerimiseks ei ole piisavalt ressursse, on mõttekas valmistada otsustustasandile ette esitlus, millega näitlikustatakse tööprotsesside mõjuanalüüsi ja riskianalüüsi tulemusi. Puuduvate ettevaatusabinõude tagajärgi peaks tutvustama vastavalt äriprotsesside prioriteetidele. Sealjuures mängivad olulist rolli nii vastava äriprotsessi kindlustatuse hetkeseis kui ka jääkrisk protsessi kindlustamatajätmise korral. Peale selle on võimalik analüüsida veel realiseerimata meetmete kulutusi ja nendega seotud töömahtu. Tekkivat riski tuleks kirjeldada ning seejärel esitada analüüs juhtkonnale otsuse tegemiseks. Pärast esitlust tuleks teha otsus nii eelarve kui ka realiseeritavate äriprotsesside prioriteetide suhtes. Kuna juhatus peab vastutama kõigi tagajärgede eest, toimuvad edasised sammud alles pärast juhatuse otsust selle kohta, kas jääkrisk on institutsiooni jaoks vastuvõetav.

6.2 Meetmete rakendamise järjekorra kindlaksmääramine

Kui olemasolevatest rahalistest vahenditest või personalist kõikide meetmete rakendamiseks kohe ei piisa, tuleb kindlaks määrata tegutsemisjärjekord. Meetmete rakendusjärjekorra kindlaks määramisel tuleb arvestada äriprotsessi turbe prioriteetidega. Lisaks tuleks arvestada järgmiste aspektidega.

- Kui äriprotsess sisaldab komponenti või osa, mille katkestus tooks kaasa kogu äriprotsessi katkestuse, peab selle kõrvaldamine või turve olema esmatähtis.

- Kui äriprotsess sisaldab üksikuid osaprotsesse, mis on märgatavalt nõrgemini turvatud kui ülejäänud osaprotsessid, siis peaks ühtlase taseme saavutamiseks olema nende protsessidega tegelemine eelisseisundis.

- Mõne meetme korral tuleneb sunnitud ajaline järjestus loogilistest sidususustest.

- Mõned meetmed on laiaulatusliku mõjuga, seevastu teised aga piiratud, kohaliku mõjuga. Tihtipeale on mõttekas jälgida esmalt laiaulatusliku mõju.

Otsused selle kohta, millised ettevaatusabinõud kohe kasutusele võetakse või edasi lükatakse ja kus jääkriske aktsepteeritakse, tuleks hoolikalt ka juriidilistel põhjustel dokumenteerida. Hilisemate vaidlusjuhtumite korral tuleks oma hoolsuskohustuste tõestamiseks küsida kolmandate isikute arvamusi ja need dokumenteerida. Spetsialistide ettepanek meetmete valimise ja järjekorra kohta tuleb esitada juhtkonnale ja lasta see kirjalikult kinnitada.

6.3 Ülesannete ja vastutuse määramine

Tuleb kindlaks määrata, kes millised ettevaatusabinõud ellu viib ja mis ajaks. Kogemustest lähtuvalt hilineb ilma selliste määratlusteta realiseerimine tunduvalt, kuni isegi selleni, et realiseerimist ei toimugi. Seejuures tuleb jälgida, et määratud spetsialistil oleks meetmete realiseerimiseks piisavalt oskusi ja ta oleks piisavalt pädev. Ka peavad tema kasutuses olema kõik vajalikud ressursid.

Samuti tuleb kindlaks määrata, kes vastutab realiseerimise järelevalve eest ja kellele tuleb meetmete realiseerimise lõpetamisest teada anda. Tavaliselt edastatakse teade hädaolukorra spetsialistile. Selleks, et keegi teine realiseerimisülesandeid ära ei võtaks, tuleks regulaarselt kontrollida, millised on meetmete realiseerimise senised edusammud.

Valmis realiseerimisplaan peaks sisaldama järgmist teavet:

- meetmete kirjeldus,
- elluviimise valmisolekukuupäevade kindlaksmääramine,
- eelarve piirid,
- rakendamise ja realiseerimise järelevalve eest vastutavad isikud.

6.4 Juurutamist saatvad meetmed

Vajalikke realiseerimist toetavaid meetmeid on ülimalt oluline õigel ajal kavandada ning realiseerimisprotsessi planeerida. Nende meetmete hulka kuuluvad eelkõige teadvustamis- ja koolitusmeetmed. Nende abil peaks töötajatele selgitama kriisihalduse vajalikust ja selle rolli.

Kui töötajaid ei ole piisavalt koolitatud, võib see hädaolukorraga toimetuleku ajal reaktsioonivõimet aeglustada. Kui töötajad tunnetavad, et neid on liiga vähe informeeritud, võib see viia negatiivsete arvamusteni .

7 Hädajuhtumi lahendamine ja kriisihaldus

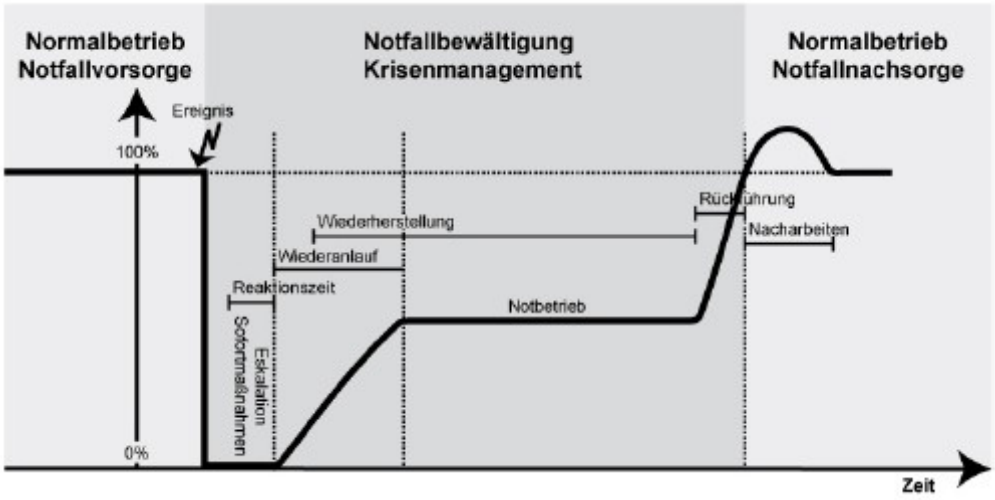
Kuna ka riski vähendavate meetmetega ei saa kõiki riske täiesti kõrvaldada, tuleb ülejäänud jääkriskide suhtes kasutusele võtta ettevaatusabinõud. Seda tehakse hädaolukorra- või kriisihalduse loomise kaudu, mis aktiveeritakse vastavalt hädaolukorrale või kriisile. See sisaldab võimalike hädaolukordade ja kriisisituatsioonide tuvastamist ja analüüsi, lahendusstrateegiate väljatöötamist ning lisaks ka üldmeetmete sissejuhatust ja nende edasist jälgimist. Kahjujuhtumi korral, mis mõjutab äritegevuse edasist jätkamist, käivitatakse vastavalt juhtumile kas lokaalne hädaolukorra lahendamine või kriisihaldus. Kriisihaldus on hädaolukorrahalduse raames osa üleinstitutsioonilisest kriisihaldusest ning kujutab endast hädaolukorraga toimetuleku kõrgemat eskalatsiooniastet.

Toimiv hädaolukorra lahendamine ja kriisihaldus nõuavad ülesehituse ja töövoo organiseerimist. Töövoo organiseerimist tutvustati peatükis 4.3.2. Kriisistaapi vajatakse nii kriisihalduse kui ka hädaolukorra lahendamise jaoks. Erinevus seisneb vastutuses ja ülesehituses. Kui hädaolukorda lahendatakse suuremalt jaolt hädaolukorraplaanidega, siis kriis nõuab teistsugust lähenemisviisi. Kriisi ainulaadsuse tõttu esitatakse kriisistaabi tööle hädaolukorraga võrreldes suuremaid nõudmisi. Seetõttu eristatakse suurtes institutsioonides mõnikord hädaolukordi ja kriisistaapide tööd nõudvaid olukordi. Lihtsuse mõttes loobutakse sellest siinkohal ja hädaolukorra staapi vaadeldakse lokaalse kriisistaabina.

Töövoo kirjeldus sisaldab tegevust pärast kahjujuhtumi teket, alustades teatest, minnes edasi eskalatsioonini ja taastamiseni ning lõpetades tavaolukorra taastamisega. Järgnevalt kirjeldatakse kriisihalduse ja hädaolukorraga toimetuleku olulisemaid struktuure ja samme. Sealjuures tuleb jälgida, et kahjujuhtumi korral ei tohi toimida jäigalt plaani järgi, vaid käitumine tuleb vastava olukorraga sobitada. See peegeldub nii aktiivsema lähenemisega organisatsioonistruktuuris kui ka struktuurisiseses töövoos.

7.1 Töökorralduse määratlemine

Hädaolukorra või kriisi tekkimisel kujunevad üldised osasammud ja ülesanded järgmiselt.



Joonis 9: Hädaolukorra ja kriisiga toimetuleku etapid

Normalbetrieb Notfallvorsonge - Tavarežiim hädaolukorraks valmisolek
Notfallbewältigung Krisenmanagement - hädaolukord lahendamine kriisihaldus
Normalbetrieb Notfallnachsorge - Tavarežiim hädaolukorra järelhooldus
Enelgnis - Sündmus
Notbetrieb - hädaolukorrarežiim
Reaktionszeit - Reaktsiooniaeg
Wederanlauf - Taaskäivitus
Zeit - Aeg

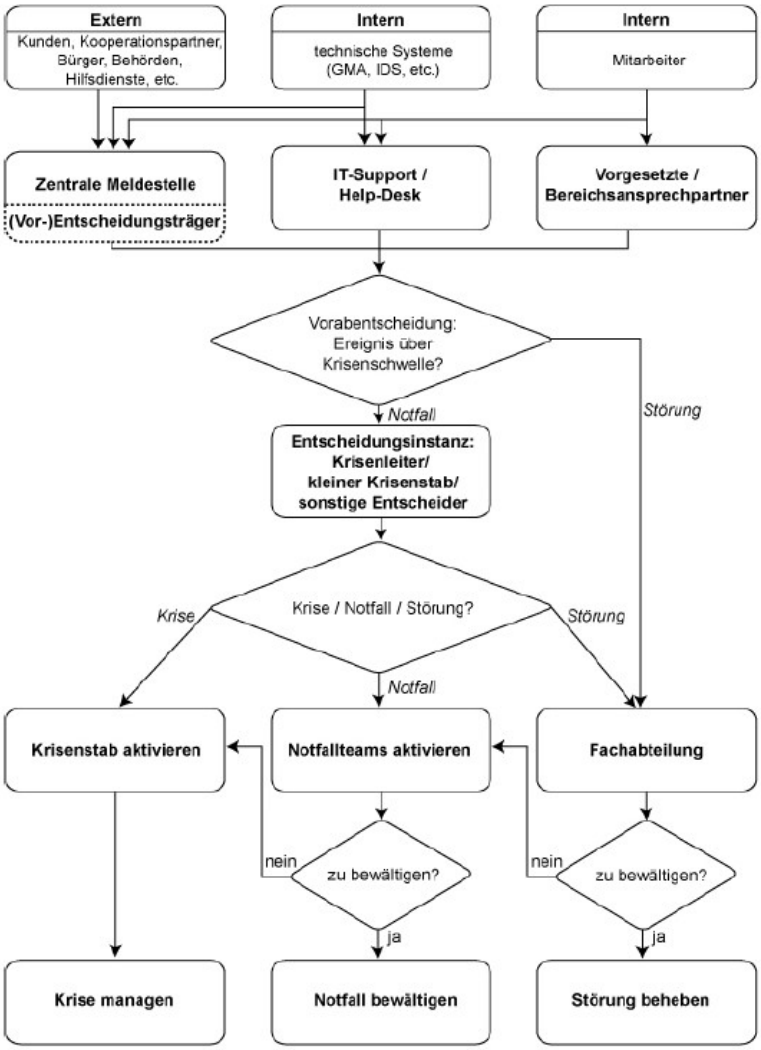
Pärast kahjujuhtumi toimumist käivitatakse vastava teatega hädaolukorraga või kriisiga toimetuleku plaani. Vajadusel rakendatakse erakorralisi meetmeid ja kui olukord ületab kindla piiri, laiendatakse haldusülesanded kriisistaabi juhile. Ta hindab olukorda, teeb kindlaks, mis

juhtus, ja milliseid tagajärgi oodata võib. Sõltuvalt juhtumi raskusest antakse ülesanne viga kõrvaldada tehnilisele osakonnale, hädaolukorraga toimetuleku jaoks teavitatakse kohalikku hädaolukorra meeskonda, kriisi haldamiseks kutsutakse kokku kriisistaap (vt joonis 10).

Kui kriisistaap kokku tuleb, siis on selle eesmärk kahju vähendada ja protsessid nii ruttu kui võimalik taastada. See jagab meeskondadele vastavaid juhiseid ning säilitab ülevaate olukorrast. Staap kindlustab nii sisemise kui ka välimise kriisikommunikatsiooni. Pärast tegevuse taastamist või tavarežiimile üleminekut taastab staap hädaolukorraeelse seisundi ning kehtima hakkavad institutsiooni tavapärase ülesehituse struktuurid.

7.1.1 Teavitamine, häire andmine ja eskalatsioon

Hädaolukorra või kriisi edukal lahendamisel on oluliseks teguriks kiire ja sobiv infovoog. Seepärast on sündmustest teavitamise, eskalatsiooni ja häiremeetodite kindlaksmääramine väga tähtis.



Joonis 10. Häire andmine ja eskalatsioon

(Extern - väline; *Intern* – sisemine; *Kunden, Kooperationspartner, Bürger, Behörden, Hilfsdienste, etc.* - Klient, Koostööpartner. elanikud, ametkonnad, abiorganisatsioonid, jne, *technische Systeme (GMA, IDS, etc.* - Tehnilised süsteemid (GMA, IDS, jne); Mitrabeiter – töötaja; Zentral Meldestelle - Keskne infopunkt; (Vor-)Entscheidungsträger - (Eel)Otsuseandja; IT-Support/Help-Desk - IT-tugi/ infolaud; Vorgesetzte/Bereichsansprechpartner Ülemus / osakonna infoisik; Vorabentscheidung: Ereignis über Krisenschwelle? – Eelotsus: juhtum üle kriisilävendi, Entsheidungsinstanz: Krisenleiter/kleiner Krisenstab/sonstige Entscheider - Otsustusinstants / Kriisijuht / väike kriisistaap; *Krise/ Notfall/ Störung* – kriis/hädaolukord/tõrge*; Krisenstab aktivieren* – kriisistaabi aktiveerimine*;Notfallteams aktivieren* – hädaolukorrameeskondade aktiveerimine*; Fachabteilung* – tehniline osakond*; zu bewältigen* – tuleb lahendada*; Krise managen* – kriisi haldama*; Notfall bewältigen* – hädaolukorda lahendama*; Störung beheben* – tõrget kõrvaldama**)**

Keskne raportikoht

Teade erakordsete või kriitiliste sündmuste kohta võib tulla nii seest kui väljast. Teated tuleb ilmtingimata kindlaks määrata, et oleks kindlustatud, et kõik teated kogutaks kokku selleks määratud keskses kohas. Sealjuures võib olla tegemist ühe või mitme kohaga (CERT, IT-tugi, retseptsioon, osakonnajuht, kooskõlastuskeskus, hädaolukordadele reageerimise keskus), kus on tegemist erinevat tüüpi juhtumitega (näiteks tulekahjuhäire, teenusepakkujate töö katkestus, finantskriis, IT-kriis). Need tuleb aga selgeks teha ja nendest tuleb kõigile töötajatele teada anda. Vajadusel tuleb juhtida teave edasi ka institutsioonist välja.

Keskne teadetekeskus peaks olema avatud ööpäevaringselt. Väljaspool tavalisi tööaegu saab seda tagada näiteks vahetuste või alltöövõtu kaudu või automaatse edastamisega valmisolekus olevale isikule.

Siseteadete korral on võimalik eristada teateid, mis pärinevad töötajatelt, ning teateid, mis pärinevad tehnilistelt süsteemidelt (näiteks häiresüsteemid). Välised häireteated laekuvad tavaliselt klientide, äripartnerite, elanike, asutuste või ka abimeeskondade kaudu.

Kindlustamaks, et esmaseks analüüsiks oleks kogu vajalik teave olemas, peaks isikute saadetud teateid keskses teadete laekumise kohas vastu võtma kindla formaadi järgi. Teated peaksid olema lühidad, oletused peaksid olema faktidest selgesti eristatavad. Teated peaksid sisaldama järgmisi andmeid:

- sündmuse koht ja aeg,
- teate edastanud isik või osakond,
- võimalikud kannatanud isikud, alad või protsessid,
- võimalikud põhjused või tekitajad ning
- hetkemõjud.

Teatud juhtudel annab keskne teabekeskus käsu erakorraliste meetmete läbiviimiseks, näiteks päästeteenistuste alarmeerimiseks või töötajate heliliseks ja/või visuaalseks teavitamiseks.

Häire- ja eskalatsiooniastmed

Niipea, kui kahjujuhtum ületab kindla piiri, laiendatakse sellega toimetulek vastutavatele isikutele. Laiendamise aluseks on nn häire- või eskalatsiooniastmed. Need on vaja varem kindlaks määrata. Lisaks tuleb defineerida kriteeriumid ja piirväärtused ning luua ka otsustusabi. Äärmuslikes olukordades võib institutsioon otsustada ainult ühe eskalatsiooniastme kasuks, st tavarežiimist minnakse koos rikkehaldusega otse üle kriisiolukorrale. Tavaliselt kasutatakse aga mitmeastmelist eskalatsioonimudelit. See võimaldab juhtumitele konkreetselt reageerida.

Eskalatsiooniastmed võivad välja näha järgmiselt.

Eskalatsiooniastmed			Näited
1	Roheline	Tavakäitus	~
2	Kollane	Veateade	Juhtumid, millest tuleb teatada, mis tuleb kontrollida ja dokumenteerida ja mis tuleb
3	Oranž	Eelhäire	Juhtumid, mille puhul on vaja rakendada esmaseid tõrjuvaid või riski vähendavaid meetmeid, näiteks üksiku tulekahju kustutamine.
4	Punane	Hädaolukord	Juhtumid, mis mõjutavad tugevalt äritegevust ning mida ei ole võimalik ettenähtud aja jooksul kõrvaldada.
5	Punane	Kriis	Kriisipotentsiaaliga juhtumid, mis ohustavad institutsiooni eksistentsi või inimelusid ning mis vajavad kõrgendatud tõhususega kooskõlastatud tegevust.
6	Punane	Katastroof	Laiaulatusliku kahjuga juhtumid, mis ei piirdu ainult institutsiooniga.

Tabel 17. Võimalikud eskalatsiooniastmed

Häire- ja eskalatsioonimeetodid

Eskalatsiooni- või häiremeetodi kindlaksmääramisel tuleb tuvastada, kes eskalatsioonikäsu annab, kellele see antakse ja kes keda alarmeerib. Vastavalt keskse teatekeskuse kvalifikatsioonile otsustab keskus abimaterjalide abil, millise eskalatsiooniastmena vastavat juhtumit käsitleda, või teavitab vastava otsuse langetamiseks mõnda otsustusõigusega isikut. Tõrke esinemise korral edastatakse teave vastavale osakonnale. Kui ületatakse kindel hädaolukorra piir, laiendatakse otsustusõigus hädaolukorra lahendamise astmele. Hädaolukorraga toimetuleku astmele võib olukorda laiendada ka tehniline osakond, näiteks IT-häirehaldus või äriprotsesside spetsialistid. Seejuures on enamjaolt tegemiste aeglaselt arenevate häiretega, mis on ületanud kindla piiri ja muutunud seega hädaolukorraks.

Kui olukorda laiendati otsustusinstantsini, peab see kõik otsused vastu võtma, olenemata sellest, kas tegemist on häire, hädaolukorra või kriisiga. Otsustusinstantsiks võib olla kriisistaabi juht, mõni teine konkreetselt nimetatud isik (näiteks juhatuse liige) või väike grupp inimesi nt kriisistaabist. Kriisistaabi juhi poolt räägib asjaolu, et seeläbi langeb veel üks eskalatsiooniaste ära ning vajalikud teadmised ja kompetentsid olukorra hindamiseks jäävad alles. Selle valiku vastu räägib asjaolu, et kriisistaabi juht võib välja kuulutada kriisi ja nõnda institutsioonis „võimu" haarata. Seda hüpoteetilist probleemi saab lahendada nii, et turvameetmena luuakse mitu kontrollinstantsi, mis saavad kriisi väljakuulutamist kontrollida, tühistada ja deeskaleerida. Käsu kontrolliks võib anda igaüks.

Kui otsustusinstantsi otsuse järgi on tegemist häirega, edastatakse teave vastavale tehnilisele osakonnale. Hädaolukorra, st lokaalse kahjujuhtumi korral, alarmeeritakse vajalikke hädaolukorra meeskondi ja kohalikku hädaolukorraga toimetuleku meeskonda, kes peaksid olukorra lahendama. Kui tegemist on laiaulatuslikuma kahjujuhtumiga, mis vajab ulatuslikku koostegutsemist ja mida ei ole võimalik ainult hädaolukorraabiplaanidega lahendada, kutsutakse kokku olukorrale kohandatud kriisistaap. Vajadusel tuleb teavitada ka teisi asutusi, näiteks filiaale, ametkondi, tervisekaitseametit. Kriisistaabi juht otsustab ka, kas kõrgemaid haldusüksusi on vaja kaasata.

Häire ja eskalatsiooni jaoks peavad olemas olema plaanid, mis kajastavad eskalatsiooniviise, kriisistaabiliikmete kättesaamist, ning informeerimist vajavaid väliseid asutusi. Plaanid sisaldavad ka juhiseid juhtumiteks, kus kriisistaabi või hädaolukorra meeskonna üksikuid liikmeid ei ole võimalik kätte saada. Olulise informatsiooni graafiline esitamine (näiteks andmevoodiagrammina) lihtsustab teabe omandamist ja parandab ülevaadet andmetest. Sellest võib eriti palju kasu olla stressisituatsioonis. Olukorraga seotud isikuid ja väliseid asutusi peaks alarmeerima võimalikult kiiresti, nii et suuremate ettevõtete või suurema hulga teavitatavate asutuste korral tuleks mõelda tehniliste abivahendite kasutamisele.

Viis

Kindlaks tuleb määrata, kuidas eskalatsioon ja alarmeerimine läbi viiakse. Seda võib teha jadana - üks isik teavitab üht või mitut teist isikut - või tähekujuliselt – inimesi teavitatakse kesksest kohast. Samuti tuleb kindlaks määrata, millisel ajahetkel informatsioon edastatakse, millal kriisistaapi teavitatakse ja millal talle häire antakse.

Alarmmerimeisel peaks järgima mõningaid põhimõtteid. Teade hädaolukorra lahendamisega seotud isikutele peaks olema lühike ja konkreetne. Alarmeerimise korral tuleks arutelusid ja olukorra pikemat selgitamist vältida. Teatest peaks olema selgesti aru saada, milliseid samme alarmeeritu ette peab võtma, nt kriisistaapi ilmuma. Alarmeeritu peab kohe reageerima. Kui alarmeeritava majapidamises elab veel isikuid, kes võivad teate vastu võtta, tuleb neid eelnevalt koolitada. Neile tuleb selgitada, mida nad häireteate korral tegema peavad. Häire andja peab häire andmise täielikult dokumenteerima, muuhulgas peab ta kirja panema järgmised andmed:

- keda alarmeeriti,
- kes alarmeeris,
- millal alarmeeriti,
- kes kätte saadi ja
- milline oli tulemus.

Häire andmine nõuab tehnilist tuge, mis tuleb kindlustada eelkõige hädaolukorra ja kriisi korral. Enamasti kasutatakse tavatelefone, mobiiltelefone, internetitelefone (VoIP), piipar,

raadio- või satelliitsideseadmed. Esmase alarmeerimise korral tuleks eelistada süsteeme, mis tuvastavad, kas isik saadi kätte ja kas teade anti edasi. SMS-i (*Short Message Service*) alarmeerimiseks kasutamine on ainult tinglikult sobilik, kuna sel juhul on võimalik tagasisidet saada ainult ajalise viivitusega ning puudub ka kindel edastusaeg.

Kuna levinumad alarmeerimissüsteemid, olgu need siis realiseeritud institutsioonisisese süsteemina või teenusena sisse ostetud, kasutavad internetivõrku, telefonivõrku või isegi mõlemat, tuleks katastroofijuhtudeks, mille korral telekommunikatsiooni ja/või interneti infrastruktuur on häiritud, mõelda alternatiivsete kommunikatsiooni- ja häireedastusmeetodite peale.

7.1.2 Kiirmeetmed

Pärast seda, kui sündmusest on teada antud, tuleb hädaolukorraga toimetulekuks käivitada kiirmeetmed. Kiirmeetmete all mõeldakse siinkohal näiteks tulekahjude kustutamist, evakueerimist või isikute päästmist. Nende meetmetega alustatakse juba enne hädaolukorra eskalatsiooni. Siinkohal on oluline vältida ajakaotuse tõttu tekkida võivaid suuremaid kahjusid, eelkõige inimkaotusi.

Vastavad juhised ja konkreetsed ülesanded tuleb juba varem kindlaks määrata ja dokumenteerida. Viivitamatute meetmete määrajad ja läbiviijad tuleb selgelt määratleda. Hädaolukorraks tuleb kindlaks määrata näiteks esmaabiandjate, parameedikute, esmaste tulekahjuga võitlejate, evakueerimisabiliste või operatiivmeeskonna koosesis. Neile antakse otsekohe häire ning nad tegutsevad sündmuskohal iseseisvalt.

Kuna on olemas vastavad, kutseühingute antud seaduslikud nõuded, mida iga institutsioon täitma peab, peaks igas institutsioonis olema vastavad juhised erakorraliste meetmete rakendamiseks. Vastavad organisatoorsed meetmed tuleb sobivas vormis hädaolukorra lahendamise töövoo reguleerimisse integreerida. Vajalikud juhised ja teave tuleb kanda kriisikäsiraamatusse.

7.1.3 Kriisistaabi ruum

Olukorra eskaleerumisel kriisiks informeeritakse kohe kõiki kriisistaabi töötajaid, kes kogunevad varem kindlaks määratud kohta, kriisistaapi. See keskus on kriisistaabi töökoht, mis peab nii asukoha kui ka varustusega seoses vastama spetsiaalsetele nõuetele.

Kriisistaabi ruumi puhul on oluline, et see oleks valitud nii, et hädaolukorra või kriisi korral oleks see kriisistaabi liikmetele kergesti ligipääsetav. Lähtuvalt institutsiooni põhiasukohast peaks see asuma kesksel kohal. Juhuks, kui põhiasukohas on kriisistaabi ruumide kasutamine võimatu, peaks olema olemas alternatiivne asupaik, mis lähtuvalt hädaolukorrastsenaariumitest peaks paiknema põhiasukohast piisavalt kaugel. Võimalusel sobivad kriisistaabi ruumideks filiaali ruumid, aga ka üüritud pind, bürookonteinerid või teised mobiilsed variandid. Kriisistaabiruumi sisustamisel peaks muuhulgas jälgima järgmisi punkte.

- Piisav ruum: ruumid peaksid sisaldama piisavalt palju töökohti, aga ka eraldatud ruume, mida on võimalik esitluste tegemiseks pimendada. Pikemateks kriisideks peaksid olemas olema söögi- ja puhkealad, WC-d, pesemisruumid ja vajadusel ka suitsuruum. Kuna olukorraspetsiifilise lisapersonali arvu suhtes ei saa öelda kindlaid numbreid, ei tohiks ruumid olla liiga väikesed.

- Ligipääs: ligipääs ruumidele peab olema võimalik ka väljaspool tavapärast tööaega.

- Turvalisus: ligipääs ruumidele tuleb kindlustada piisava ligipääsukaitsega. Sõltuvalt kriisist mängib siseneva informatsiooni ja nõupidamiste konfidentsiaalsus suuremat või väiksemat rolli. Sellest lähtuvalt peaks kriisistaabi ruum olema selline, kus ei oleks võimalik väljast sisse näha. Vajadusel peaks ruum olema ka pealtkuulamiskindel.

- Tehniline sisustus: teabe hankimiseks, töötlemiseks ja kuvamiseks on vaja vastavat tehnilist varustust, mille hulka kuuluvad omavahel võrguühenduses olevad arvutid, videoprojektorid, skannerid, koopiamasinad, printerid ning kaasaskantavad mäluseadmed informatsiooni vahetamiseks ja transpordiks. Kriisistaabiruumi IT-infrastruktuur peaks intranetist, mis ei ole enam võibolla kättesaadav, sõltumatu olema, st see ei tohiks sõltuda meiliserverist, avalike võtmete infrastruktuurist või ka vajaliku teabe andmebaasidest. Mõistlikeks abivahenditeks on ka faksiaparaat, raadio, televiisor või videomakk. Lisaks tavatelefonidele peaksid olemas olema mobiiltelefonid ja vajadusel ka vooluvõrgust

sõltumatud analoogtelefonid. Katastroofiks, mille korral telefonivõrgud rivist välja langevad, peaksid olemas olema satelliittelefonid.

- Kliimaseade: parandab töökeskkonda ning vähendab lisastressi. Kliimaseadet peab olema igal ajahetkel võimalik reguleerida.

- Redundantne vooluvarustus: seadmete ja telefonide tarvis peaks olema sisse seatud redundantne vooluvarustus.

- Redundantne telekommunikatsiooni- ja internetiühendus: et internetist pärinev teave või internet ise oleks kättesaadav, tuleb kindlustada internetiühenduse redundantsus. Hoolitseda tuleb ka selle eest, et erinevaid kommunikatsiooniviise oleks võimalik kasutada.

- Muu sisustus: tehnilise varustuse kõrval on vaja ka büroomaterjali, tarbematerjali (näiteks printeri tindipadrun, patareid), töövahendeid teabe esitamiseks (näiteks tahvlid, pabertahvlid) ja informatsiooni töötlemise ja hankimise varustust (näiteks kaardid, teatmeteosed, telefoniraamatud). Konfidentsiaalsete dokumentide hävitamiseks peaks olemas olema ka paberihunt. Vastavalt identifitseeritud kahjujuhtumitele (näiteks kemikaalide vabanemine) võib vajalik olla kaitsevarustuse olemasolu.
- Varustamine ja jäätmekäitlus: lahendada tuleks nii varustuse kui ka jäätmekäitluse

küsimus.

Ruumi ja selles oleva varustuse funktsionaalsust tuleb regulaarselt kontrollida.

Eriliseks väljakutseks on kriisid, mille korral on kriisistaabi liikmete kriisistaabiruumis töötamine võimalik ainult piiratud määral. See on ebaotstarbekas, lausa ebasoovitatav, näiteks pandeemia korral. Selliseks juhuks tuleb välja töötada alternatiiv, mis võimaldab eraldatud olemist, kuid koos töötamist.

7.1.4 Kriisistaabi ülesanded ja kompetentsid

Kui sündmus eskaleerus ja kriisistaap aktiveeriti, algab selle kokkutulekuga kriisistaabiruumis tegelik hädaolukorra või kriisi lahendamine. Kriisistaap määratleb kahjustatud ala (näiteks hoone, filiaal, mitu asukohta). Kriisistaabi otsustusõigus kehtib ainult selle piirkonna suhtes.

Kriisistaabi põhiülesannete hulka kuuluvad otsuste tegemine, hädaolukorra meeskondade koordineerimine ja hädaolukorra või kriisiga toimetulek. Hädaolukorra ja kriisi põhiline erinevus seisneb selles, et hädaolukorda on võimalik lahendada hädaolukorraplaanidega. Kriis nõuab lisakompetentsi. Kriis on ainulaadne, seda ei ole võimalik määratleda varem olemasoleva mustriga ja kriisiolukorras on vaja teha kiireid ning kompetentseid otsuseid.

Kriisistaabi põhiliste ülesannet hulka kuulub: teabe

hankimine,

- analüüsimine ja järelduste tegemine, hetkeolukorra

- väljaselgitamine ja hindamine,

- tegevuskavade väljatöötamine ja hinnangute andmine seoses eduga, olukorrast tulenevate riskidega ja raamtingimustega,

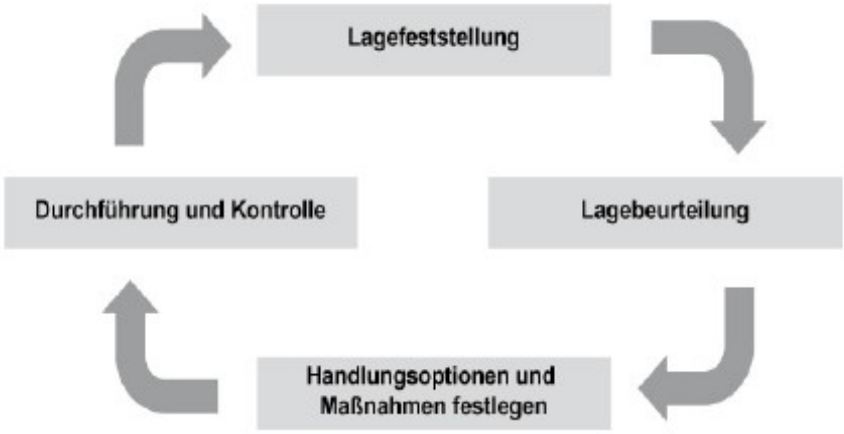
- meetmete kindlaksmääramine,

- hädaolukorra meeskondadele meetmete läbiviimise ja kontrollimise käskude jagamine,

- meetmete tõhususe kontroll ja vajadusel korrigeerimine, kui need ei too soovitud tulemust, ja

- partnerite, töötajate, ametkondade ning meediaga suhtlemine.

Pikema hädaolukorra puhul peab kriisistaap oma tegevuse ja struktuuri, aga ka vajaliku infrastruktuuri, ise organiseerima. Siia hulka kuulub muuhulgas ka vahetuste koostamine ning varustatus toiduainete ja tarbekaupadega.



Lagefeststellung - Olukorra kindlaksmääramine
Durchführung und Kontrolle - Läbiviimine ja kontroll
Lagebeurteilung - Olukorra hindamine
Handlungsoptionen und Maßnahmen festlegen - Tegevuskavade ja meetmete kindlaksmääramine

Joonis 11. Toimetulekuprotsess

Olukorra kindlaksmääramine ja teabe hankimine

Olukorra kindlaksmääramiseks vajatakse hulgaliselt informatsiooni. Olukorras on vaja kirjeldada tegureid ja tingimusi, mis kahjujuhtumit ja kahjutõrjet määratlevad, näiteks mõju liik ja ulatus, kahjud ning nende ennustatav areng, kannatanute arv, hetkeohud, sündmuse juhtumisaeg, varustatus- ja liiklusvõrgustiku olukord.

Et endale olukord selgeks teha, kogub kriisistaap või abipersonal kokku kogu juhtumi kohta käiva olulise teabe. Selleks on oluline, et olemas oleks võimalikult täpne pilt juhtumi tüübist, ulatusest ja sündmuste kulgemisest. Lisaks vajatakse teavet juba rakendatud meetmete kohta ning nende mõju kohta olukorrale.

See teave võib olla kriisistaabi poolt välja selgitatud, see võib pärineda kasutatavatest dokumentidest või sisse tulnud teadetest. Teated võivad pärineda nii koolitatud isikutelt, enda personalilt, luuresalkadelt, välistelt abilistelt, kui ka elanikkonnalt. Teadete töötlemisel on abiks, kui nende koostamisel jälgitakse järgnevaid põhimõtteid.

- Teated peaksid olema selged, asjalikud ja lühidad, aga samas terviklikud.
- Teated peavad olema aktuaalsed ja nad tuleb seega kohe edastada. Üles tuleb märkida juhtumi märkamise aeg.
- Toimunu kirjeldus ei tohi olla ei üle- ega alahindav.
- Peaks olema aru saada, kuidas ja tänu kellele juhtum kindlaks tehti: tänu enese tajule või kolmandate isikute kaudu. Faktid ja oletused peavad olema selgelt eraldatud. Teate saatmiskoht peaks olema tuvastatav.

Olukorra kindlaksmääramisel on üksikud teated olulise tähtsusega. Neid tuleb vastavalt saatjale erinevalt hinnata, eriti vastandliku informatsiooni korral. Olukorra ülevaate koostamisel tuleb seega arvestada teadete laekumise järjekorraga ning isikutega, kellelt need teated laekusid.

Vastavalt olukorrale võib hinnangu tegemise seisukohast olla huvitav ka lisateave, näiteks ruumipaigutuse ja geograafilise asukoha kohta, klimaatilised raamtingimused või informatsioon kannatada saanud inimeste kohta. Selleks vajab kriisistaap ligipääsu materjalidele, mida kasutavad tavarežiimis erinevad organisatsiooniüksused. Siia hulka kuuluvad näiteks hooneplaanid, plaanid ruumide asetuse kohta, plaanid ruumide kasutuse kohta, ülevaade varustusliinidest (elekter, gaas, vesi) ja informatsiooni- ning kommunikatsiooniteenuste võrguplaanid. Tuleb kindlustada, et kriisistaabil oleks alati kasutada kõige ajakohasem versioon.

Olukorra hindamine

Kriisistaap võtab olemasoleva informatsiooni põhjal vastu ühise seisukoha hetkeolukorra ning veel toimuda võivate järelsündmuste suhtes. Võimalikud küsimused olukorra hindamisel on järgmised.

- Mis võib veel juhtuda? Mis võib veel hiljem juhtuda?
- Milliseid mõjusid võib oodata?
- Kuidas on võimalik kahju edasist levikut piirata?
- Kuidas on võimalik juba tekkinud kahju kõrvaldada?

Tegevuskavad ja meetmete kindlaksmääramine

Konkreetse situatsiooniga toimetulekuks luuakse võimalikud tegevuskavad vastavalt olukorra hinnangule. Neid variante hinnatakse nende edu tõenäosuse suhtes, kaalutakse omavahel positiivseid ja negatiivseid külgi, hinnatakse tõhusust ja võimalikke positiivseid ja negatiivseid tagajärgi ning tegevusriske, mida kasutusele võetud hädaolukorrameetmed endaga kaasa tuua võivad. Tähtis on kindaks määrata strateegia, kuidas kriisiga toime tulla, ning leida õiged vahendid õigel ajal ja õiges kohas. Siinkohal tuleb arvestada hädaolukorra esmaabi strateegilisi eesmärke ja kriisihalduseks kasutatavaid ressursse.

Otsus kindlate tegevuskavade ja seega kindlate meetmete kasuks tehakse kriisistaabis üheskoos. Kiire kokkuleppe saavutamiseks on vaja teha konstruktiivset koostööd. Kui kriisistaabi liikmed ei saavuta kokkulepet, teeb otsuse kriisistaabi juhataja.

Äritegevuse jätkamisel on üks esimesi otsuseid vajalike hädaolukorrameeskondade väljaselgitamine ja nende aktiveerimine. Muuhulgas tuleb otsustada, millised omavahel ühtlustatud osaplaanid aktiveeritakse ja millised konkreetsed meetmed seega kasutusele võetakse.

Tähtis on ka otsus isiku kohta, keda teavitatakse institutsioonisiseselt, aga veelgi olulisem on, keda teavitatakse väljaspool institutsiooni. Kriisistaap, ja viimase instantsina kriisistaabi juhatus, otsustavad vastavate meetmete kasutamise üle ja jagavad vastavaid juhiseid.

Meetmete läbiviimine ja kontroll

Olukorra hindamisel väljatöötatud lahendus tuleb jagada üksikuteks ülesanneteks. Kriisistaap edastab juhised meetmete rakendamiseks erinevatele hädaolukorra- ja abimeeskondadele, kes sobivad põhjuste ja tagajärgede kõrvaldamiseks. Ta jälgib, et meetmed viidaks viivitamatult ellu.

Kasutusele võetud meetmete mõju tuleb regulaarselt kontrollida ja meetmete tõhusust tuleb hinnata. Hetkeolukorda tuleb antud teabe põhjal regulaarselt hinnata ja aktuaalne teave tuleb kanda olukorra hinnangusse. Olukorra taashindamine viib niikaua lisameetmete realiseerimiseni, kuni normaalolukord on saavutatud.

Vahetustega töö ja vahetuse üleandmine

Kriisihaldus on stressirikas ning nii füüsiliselt kui ka vaimselt kurnav. Seetõttu peaks kriisistaabi töö toimuma vahetustes. Üks vahetus ei tohiks kesta kauem kui 8 tundi, sest vastasel juhul hakkab keskendumisvõime langema. Sellest lähtuvalt tuleb luua mitu meeskonda ja reguleerida ka vahetustega töö organisatoorne kulg.

Vahetustega töö organiseerimiseks on põhimõtteliselt kaks erinevat mudelit: inimeste pidev vaheldumine või kogu meeskonna korraga väljavahetamine. Pideva vahetuse eeliseks on, et kriisistaabis on teave hetkeolukorra kohta pidevalt olemas. Samas nõuab iga väljavahetamine informatsiooni üleandmist ning põhjustab sellega grupis pidevalt rahutusi. Samas on võimalik üleminekuperioodil edasi töötada. Sellega on selged ka kogu väljavahetamise eelised ja puudused: Eeliseks on, et esineb vähem rahutusi, kuna vahetuse vahetumise kohta on ainult üks üleandmisfaas. Teisest küljest aga läheb vahetusega kaduma palju taustteadmisi hetkeolukorra ja kriisiga toimetuleku kohta. Veel üheks puuduseks on asjaolu, et üleandmisfaasis ei tegele terve kriisistaap või suur osa sellest üleüldse kriisiga toimetulekuga.

Üleandmisfaas ei tohiks olla pikem kui 15 kuni 20 minutit. Selle aja jooksul tuleb välja vahetada kogu vajalik ja tähtis teave. See sisaldab ülevaadet hetkeolukorrast, tehtud otsuseid ja läbiviidud, sissejuhatatud ja veel rakendamata meetmeid. Pärast seda peavad kõik staabi liikmed olema olukorra suhtes samal informatsioonitasandil. Kriisistaabi liikmed, kellel on spetsiaalsed ülesanded või roll, annavad oma teadmised olukorrast isiklikult järgmisele vahetusele üle. Kiire üleandmise võimaldamiseks tuleks planeerimisfaasis kindlaks määrata kriteeriumid ja käitumisjuhendid.

Deeskalatsioon

Kui hädaolukord või kriis on üle elatud, toimub deeskalatsioon, st kriisistaap saadetakse ametlikult laiali ja selle erivolitused lõpetatakse. Nagu eskalatsiooni jaoks, tuleb ka deeskalatsiooni jaoks kriteeriumid defineerida. Rakendatakse tavarežiimile üleminekuks vajalikud meetmed ja töö läheb ole tavalisele organisatsioonistruktuurile.

7.1.5 Tööprotsessidega jätkamine, taaskäivitamine ja taastamine

Hädaolukorraga toimetuleku ja kriisihalduse peamine eesmärk on äritegevuse jätkamine. Oluline on puudutatud äriprotsessid nii ruttu kui võimalik jälle töökorda seada. Äritegevuse jätkamine sisaldab konkreetseid meetmeid ja meetodeid, mis võimaldavad äritegevust eelnevalt määratud taaskäivitusaja raames taas käivitada. Hädaolukorrarežiim võib olla vähendatud ressurssidega töötav „tavarežiim", varuressurssidega vähendatud jõudlusega töö või alternatiivne töö.

Kui äriprotsess katkestati, võib parimal juhul jätkata äritegevust kahjustamata ressursside taaskäivitamisega. Kui ressursid hävitati või ei ole neid mõnel muul põhjusel enam võimalik kasutada, tuleb nad taastada. Sõltuvalt ressurssidest tähendab see seda, et need tuleb asendada, uuesti installeerida ja sisse seada.

Hädaolukorraga toimetulekul analüüsitakse hetkesituatsiooni ja võetakse vastu otsus, millised alternatiivsed äritegevuse jätkamise meetodid on üksikute protsesside seisukohast võimalikud, otstarbekad ja üldist olukorda vaadeldes ka kõige paremad ja kiiremad.

Niipea, kui kõik taastamis- ja taaskäivitusmeetmed on läbi viidud, tuleks, sõltumata sellest, kas need meetmed olid edukad või mitte, edastada teade ka kriisistaabile Tavarežiimile ei ole võimalik üle minna enne, kui kõik taastamisplaani punktid on edukalt realiseeritud. Institutsioon jääb siis ikkagi hädaolukorrarežiimi faasi.

7.1.6 Tavaolukorra taastamine ja hädaolukorrajärgne analüüs

Kui kõiki ressursse saab äriprotsesside tavarežiimiks jälle kasutada, tuleb hädaolukorrarežiim üle viia tavarežiimiks. Kuna arvestada tuleb ka äriprotsesside vaheliste sõltuvustega, tuleks äriprotsesside vaheliste või sisemiste erinevuste vältimiseks pöörduda tavarežiimile tagasi korrastatud moel. Seetõttu peab kriisistaap kindlaks määrama, millises järjekorras ja millisel ajahetkel üksikud äriprotsessid tavarežiimile üle viiakse ning seda üleviimist ka koordineerima. Nõnda välditakse suuri probleeme, mis võivad viia äritegevuse järjekordse kokkuvarisemiseni.

Enamjaolt jäädakse vähendatud ressurssidega hädaolukorrarežiimi tõttu tööplaanist maha. Et seda mahajäämist kontrollitult ning viivitamatult tasa teha, peaks äri jätkamise plaanides olema igas organisatsiooniüksuses määratud vastutavad isikud, kes koostavad ülevaate mahajäämistest ning määravad kindlaks plaani, millega töökavale järgi jõuda. Töökavale järgijõudmise plaani koostamisel tuleb arvestada hetke töökoormusega, töökoormusega hädaolukorrarežiimi ajal ning tööõiguse sätetega. Strateegilised nõuded, kuidas tööst mahajäädud aeg tasa teha (näiteks ületundidega, vahetustega tööga või lisapersonaliga), peaksid olema hädaolukorraks valmisoleku plaanis kindlaks määratud ning kooskõlastatud töötajate esindajaga.

Järeltöid peaksid jälgima vastavate organisatsiooniüksuste hädaolukorra koordinaatorid. Tuleb kindlaks määrata, kes, millisel ajahetkel ja kellele järeltööde seisust aru annab.

7.1.7 Hädaolukorra lahendamise analüüs

Pärast hädaolukorraga toimetuleku lõppu ja deeskalatsiooni tuleks hädaolukorraga toimetulekut analüüsida. Nii tuvastatud nõrkade kohtade alusel tuleks sisse viia parandusmeetmed. Analüüsi peaks läbi viima koostöös hädaolukorra spetsialistiga, kaasatud hädaolukorra koordinaatoritega ja hädaolukorraga toimetuleku eest vastutavate isikutega. Sealjuures töötatakse välja parandusettepanekud.

Hädaolukorra lahendamisel võib ka selguda, et organisatsioonistruktuurid, IT-süsteemid või äriprotsessid vajavad täiustamist. Sellistel juhtudel peaks hädaolukorra spetsialist vastava ala eest vastutavate isikutega kohtuma. Koos tuleks välja töötada parandusettepanekud. Näiteks võib olla otstarbekas teha muudatusi tulekaitses ja informatsiooniturbes.

Parandusettepanekute realiseerimiseks tuleb ametisse realiseerimisspetsialist ning kindlaks tuleb määrata realiseerimistähtajad. Hädaolukorra spetsialist peaks jälgima parandusmeetmete õigeaegset realiseerimist ja etteantud ajavahemike tagant institutsiooni juhtkonnale aru andma. Puuduste korral peab vastav vastutav organisatsiooniüksus kasutatud plaane ja meetodeid täiustama ja aktualiseerima. Uute realiseeritud meetmete ja meetodite funktsionaalsust ja tõhusust tuleks kontrollida õppuste käigus.

Lisaks parandusettepanekutele tuleb hädaolukorraga toimetuleku järeltöötlusel koostada kokkuvõttev tegevusaruanne, mis aegsasti ja „usaldusväärsena" juhatusele üle antakse. Aruannet kasutatakse muuhulgas ka selleks, et hinnata võimalikke õiguslikke tagajärgi, mis institutsioonile või üksikutele isikutele hädaolukorra või kriisi tõttu tekkida võivad.

7.1.8 Hädaolukorra lahendamise dokumentatsioon

Hädaolukorra ja kriisi lahendamise jooksul tuleb õiguslikest alustest lähtuvalt kõik olulised läbiviidud tegevused ja otsused nn tegevuspäevikus dokumenteerida. Lisaks peaks koguma teadete sisenemis- ja väljumisandmeid ning pidama kriisistaabitöötajate kohalolekunimekirja. Seda võib teha nii elektrooniliselt kui ka paberil.

Dokumenteerima peaks sellisel viisi, et kriisistaabi töötajatel ning eelkõige kriisistaabi juhil oleks kiiresti võimalik saada ülevaade hetkeolukorras. Dokumentatsiooni on vaja olukorra hindamiseks, aga lisaks veel ka hädaolukorra hilisemaks hindamiseks, st hädaolukorraga toimetuleku protsessi hindamiseks ja parandamiseks. Vajadusel tuleb salvestustest esitada ja läbi suruda nii finantseerimis-, kindlustus- kui ka õigusküsimused. Dokumenteerida tuleb muuhulgas järgmised punktid:

- kriisistaabi töö aeg,
- olukord (olemus, maht ja sündmuste kulg),
- kõik tehtud otsused, nendes osalenute nimed ja rollid ning
- otsustatud meetmed, teostuse eest vastutavad, valmimistähtajad ja teostuse seis (ülesannete jälgimine).

Standardiseeritud ankeedid ja eeltrükid, näiteks sisenemis- ja väljumisteadetele, tegevuspäevikutele või teateprotokollidele, võivad kindlustada kriisiolukorras piisava ja täpse dokumentatsiooni. Abivahendid tuleb juba enne kriisi välja töötada ja üksteisega ühtlustada.

Pärast kriisiga toimetulekut peavad kõik kriisistaabi liikmed dokumentatsioonile alla kirjutama ja kindlustama selle nõuetekohase säilitamise.

7.2 Kriisistaabi töö psühholoogilised aspektid

Iga kriis tähendab osalistele väga suurt vaimset stressi, kuid samas on tegemist keeruka lahendamist vajava probleemiga. Kriisid on ainulaadsed, dünaamilised, keerukad, ja peale selle on neil veel palju muutujaid ja parameetreid. Tänapäeva süsteemide laialdane võrgustatus raskendab ülevaate säilitamist üksikute osade tegevusest, kaskaadiefektidest ja otsuste kõrvalmõjudest. Nendes raskendatud tingimustes tuleb teha ulatuslike otsuseid, mis ei ole seotud ainult rahaliste mõjudega, vaid võivad otseselt või kaudselt mõjutada ka inimelusid.

Stressi põhjused kriisisituatsioonis on erinevad. Nendeks võivad olla juhtunust põhjustatud šokk, hirm iseenda läbikukkumise ees, hirm lähedaste pärast, emotsionaalne pinge, hirm tundmatu ees, liigne informatsioonivoog, vastandlik teave, ebapiisav informatsioon, ajahäda, segavad keskkonnatingimused nagu lärm, soojus või külm, hektilisus, nälg, janu või unepuudus. Keha reageerib sellele mõttevõime vähendamise ning kehaliste vastureaktsioonide käivitamisega. Keha toodab rohkem adrenaliini, vererõhk tõuseb, tekivad pinged, peavalu ja südame- ning vereringehäired. Stress võib põhjustada kiirustamist, keskendumishäireid, unustamist, ringmõtlemist, minestamist, üleliigset reageerimist, ebapiisavat probleemianalüüsi ja piiritletud vaatevälja ning taju. Stress võib põhjustada agressiivsust ja isegi täieliku kontrollikadu enese üle.

Samas ei ole stress mitte ainult negatiivne, vaid võib mõjuda ka positiivselt. Stress võib motiveerida ennast ületama ja edasi tegutsema. Seepärast peab kriisistaabi tööks valmistudes ka nende teguritega arvestama. Sellepärast peaksid kriisistaabi liikmed teatud määral juba algusest peale stressi suhtes vähem tundlikud ja enesekindlamad olema. Mõttekas on ennetavate ettevaatusabinõude rakendamine. Siia hulka kuuluvad näiteks järgmised.

Erialased koolitused tõstavad enesehinnangut ja vähendavad stressi, mis võib tekkida näiteks ebakindlusest.

Teadmised üldiste probleemilahendusstrateegiate kohta ning iseenda oskused ja tegutsemisviisid võimaldavad otsuseid kiirest ja korrastatult langetada.

Koolituste kaudu on kriisistaabi töötajaid võimalik ette valmistada, tõsta nende stressitaluvust, vajadusel õpetada, kuidas stressi spetsiaalsete tehnikate abil vähendada ja positiivsusesse suunata ning kuidas stressisituatsioonides emotsioone vähendada. See võib stressispiraali vältimisel oluliseks sammuks osutuda, kuna stressist tingitud valed hinnangud ja otsused põhjustavad veel rohkem stressi, mis omakorda viib jällegi väärotsuste tegemiseni.

Kriisistaabitöö psühholoogiliste ja grupidünaamiliste aspektide täiendusõpe tõstab kriisistaabi kostöö efektiivsust.

Õppustega meeskonna kriisiolukorras töötamiseks ettevalmistamine aitab luua ühiseid töömeetodeid ning ühist mõtteviisi. Sellised tegurid nagu tuttavlikkus, ühise keele loomine kriisistaabi kommunikatsiooniks, hea töökliima ja võime teisi meekonnaliikmeid teatud määral hinnata vähendavad stressitaset.

Väliseid stressifaktoreid on võimalik vähendada positiivse töökliima ja -tingimuste (näiteks toitlustamise, ruumi sisekliima, puhke- ja magamisvõimaluste) loomisega.

7.3 Kriisiaja kommunikatsioon

Kriisikommunikatsioon on üks hädaolukordade halduse edu faktoreid. Kriisikommunikatsioon on kriisi ajal ning pärast kriisi toimuv suhtlus erinevate huvigruppidega. Selle eesmärgiks on kriiside likvideerimine, edasise kahju ärahoidmine, inimeste teavitamine ning usaldus- ja mainekahjustuste ärahoidmine. Eristada võib organisatsioonisisest ja -välist kriisikommunikatsiooni. Käesolevas dokumendis käsitletakse kriisikommunikatsioonina igasugust kommunikatsiooni, mis on seotud hädaolukorra või kriisi likvideerimisega. Organisatsioonivälise kriisikommunikatsiooni eesmärgiks on informeerida. Seejuures leiab sihtgruppe nii organisatsiooni seest kui ka sellest väljastpoolt.

7.3.1 Organisatsioonisisene kriisikommunikatsioon

Organisatsioonisisese kriisikommunikatsiooni juurde kuuluvad teavitamine, eskalatsioon ja alarmeerimine, aga ka igasugune kommunikatsioon, mis on seotud teabe hankimisega, hädaolukorrameeskondade koordineerimine või kriisi lahendamiseks väliste osapooltega

koostöö tegemine. Väliste osapoolte hulka võivad kuuluda näiteks äripartnerid, kliendid, päästeteenistus, abiorganisatsioonid, tuletõrje, politsei või *Technisches Hilfswerk.*

Kui kriisijuhtum ei ole organisatsioonisiseselt piiratud, võib kahjuleviku piiramiseks osutuda vajalikuks informeerida väliseid osapooli (nt äripartnereid või kliente), kes samuti võivad olukorrast puudutatud olla, ning nendega koostööd teha. Turbekriitilise juhtumi korral võib see tähendada, et organisatsiooniväliste kontaktidega tuleb läbi arutada turbeprobleemid ning vastumeetmed tagajärgede piiramiseks. Kui teabeedastust ega koostööd ei toimu ja informatsioon turbeprobleemide kohta jõuab koostööpartneriteni teiste kanalite kaudu, võib see edasist koostööd välispartneritega negatiivselt mõjutada ja olemasolevaid usaldussidemeid kahjustada.

Organisatoorsete määratluste kõrval, kes, kellele, millal teada annab, olukorda laiendab, alarmeerib (vt peatükk 7.1.1) ja informeerib, tuleb kindlaks määrata,

- kes vastutab hädaolukordade halduses osapoolte ja rollide vaheliste informatsioonivoogude eest,
- millal ja milliste ajavahemike tagant teateid edastatakse ja
- kuidas kommunikatsioon toimub.

Siia kuuluvad näiteks informatsioonivoogude liikumine juhtumi tegevuspaigast või hädaolukorrameeskondadelt kriisistaapi ja tagasi. Olulist tähelepanu peaks pöörama ka kriisikommunikatsiooni tehnilistele ja logistilistele aspektidele. Seejuures tuleb vastata järgmistele küsimustele.

- Millised on hädaolukorraga toimetulekuks kasutatavad sidevahendid (kõne, tekst, andmed, video ja pildid)?
- Millised sidesüsteemid (lõppseadmed ja ühendused) on põhimõtteliselt ja alternatiivina erinevates paikades olemas?
- Milline on üksikute sidesüsteemide rivist väljalangemise risk?
- Millised meetmed tuleb, lähtuvalt kommunikatsioonisüsteemide kättesaadavuse nõuetest hädaolukorra ajal, kasutusele võtta?

Kriisiolukordades on vaja suhelda kindlalt ja turvaliselt, mistõttu tuleb kriisiperioodil kindlustada kommunikatsioonisüsteemide kättesaadavus. Võimalike ennetavate meetmete hulka kuulub piisav arv lõppseadmeid, kindlustatud vooluühendus lõppseadmete jaoks ja eriti ka alternatiivsete kommunikatsioonivõimaluste kasutamisvõimalus (näiteks internet, püsiühendus, mobiiliside, seteliitside). Süsteemide valimisel peaks arvestama ka suhtluse konfidentsiaalsuse ja terviklusega ning samuti peaks mõtlema kommunikatsioonipartnerite autentimisele.

7.3.2 Organisatsiooniväline kriisikommunikatsioon

Kuna kriisi, hädaolukordade halduse ja juhtkonna käitumise tajumine on avalikkuses suhtes määravaks faktoriks, siis kujutab iga kriis endast ka kommunikatsioonikriisi. Kriisi leviku üle otsustab avalikkus. Oluline on ära hoida ulatuslik paanika, emotsioone piiritleda ja hirmudel mitte tekkida lasta. Seepärast on tähtis, et organisatsioonivälise kriisikommunikatsiooni (kriisisuhtekorralduse) jaoks oleks määratud kindel vastutus ning strateegia.

Organisatoorsed struktuurid

Välise kriisikommunikatsiooni eest vastutab ainuüksi kriisistaabis olev kriisikommunikatsiooni juht. Kogu suhtlus meediaga peaks käima tema kaudu või tema juhiste järgi. Kriisikommunikatsiooni juhti saavad aidata töötajad, kes võtavad enda peale spetsiaalsed ülesanded, nagu kontakti hoidmine meediaasutustega, pressikonverentside juhtimine ning *online*-teabe toimetamine. Kriisikommunikatsiooni meeskonnas on abiks järgmised rollid: pressiesindaja, kes astub avalikkuse ette, ekspert, kes analüüsib teaduslikke ja asjakohaseid küsimusi, õigusekspert õigusküsimusteks ning pressi- ja suhtekorraldusekspert, kes vastutab meedia jälgimise eest.

Selleks, et nad oleksid võimelised ettenägematutele küsimustele vastavalt reageerima ja suurele ajapingele ja stressile vastu pidama, peaks välise kriisikommunikatsiooni meeskonna liikmeid oma tegevuseks treeningute ja koolitustega (näiteks meediatreening) ette valmistama. Nad peavad õppima, kuidas end mõtlematutest ütlustest mitte provotseerida lasta ning

rahulikuks jääda. Vastamisi peab seisma küsimustega, mis tihtipeale käsitlevad organisatsiooni vigu. Neile vastates ei tohi kunagi agressiivselt reageerida. Kriisikommunikatsioon on väga nõudlik ja keerukas ülesanne. Selle professionaalseks läbiviimiseks vajatakse spetsialiste. Sellealaseid koolitusi viiakse muuhulgas läbi ka kriisikommunikatsioonile spetsialiseerunud agentuurides.

Kui kasutamiseks ei ole piisavalt sisemisi ressursse, tuleks mõelda, kas ei oleks kriisi korral mõttekas kaasata välist kriisikommunikatsioonieksperti. Vastav isik tuleks juba varem välja valida, lepinguliselt siduda ning institutsiooni ning selle terminitega tuttavaks teha.

Tuleb kindlustada, et kriisikommunikatsiooni juhil oleks piisavalt andmeid kriisiolukorra, võimalike kahjude, läbiviidud ja plaanitud vastumeetmete (ilma detailideta) ja juba teavitatud üksuste kohta. Ta kontrollib ja lubab avaldada kogu teavet, mis on kriisiga seotud ning mida informeerimise tarbeks edastatakse. Kui juhtkonna esindaja on seotud kriisikommunikatsiooni ülesannetega, näiteks tähtsate huvigruppidega kontakti hoidmisega, tuleb arusaamatuste ennetamiseks tema ülesanded ja kompetents kindlaks määrata.

Kommunikatsioonistrateegia

Kindlaks tuleks määrata kindel kommunikatsioonistrateegia, mis garanteerib kriisi korral sisulise ning ühtse tegutsemise. Kriisikommunikatsioonistrateegia määrab suhtluse ja keelekasutuse raamistiku ning põhimõtted. See määrab kindlaks, kes koostab kriisikommunikatsiooni jaoks vajaliku teabe, milline sihtgrupp millise info saab ning millist informatsioonitasandit millisel kriisihetkel millise meediumi kaudu edastatakse. Seda strateegiat tuleb kriisikommunikatsiooni plaanis täpsustada.

Kriisikommunikatsioonistrateegia väljatöötamisel on abi sellest, kui tuvastatakse kriisi jaoks olulised huvigrupid, nende vajadused, väärtused, eesmärgid ja võimalik huvi teabe vastu. Selle aluseks võiks olla hädaolukordade halduse loomisel läbi viidud huvigruppide analüüs. Peale juba eespool nimetatud huvigruppide nagu osanikud, investorid, juhatus, töötajad, tarnijad ja kliendid mängivad kriisikommunikatsioonis olulist rolli ka teised huvigrupid. Sinna hulka kuuluvad näiteks perekonnaliikmed, elanikud, otseselt puudutamata avalikkus, järelevalveasutused, poliitilised esindajad, konkurendid, keskkonnaühendused, kodanikuinitsiatiivid, protestigrupid ja eelkõige erinevad meediaasutused. Gruppe võib jagada institutsioonisisesteks, otsesteks, kaudseteks, asjassepuutuvateks ekspertideks ja veel teisteks huvigruppideks (vt joonis 12).

Joonis 12. Kriisikommunikatsiooni sihtgrupid
Sprecher Krisenmagagement -hädaolukordade halduse pressiesindaja; Management – juhatus; Mitarbeiter – Töötaja; Angehörige – elanik; Konkurrenten - Konkurendid; Medien – meedia Öffentlichkeit – avalikkus; Bürgerinitiativen – kodanikualgatused; *Investoren - Investorid (Umweltverbände* – keskkonnaühendused*; Dienstleister* – teenusepakkujad*; Lieferanten* – tarnijad*)*
Analüüsi eesmärgiks on tuvastada huvi kriisi kohta käiva informatsiooni vastu ning välja selgitada gruppide motiivid. Samuti on vaja välja töötada strateegiad ning meetmed nende gruppidega suhtlemiseks. Analüüsi on mõttekas sisse arvestada ka erinevate huvigruppide

mõjuvõim ja nende võimalused sanktsioonide kehtestamiseks (näiteks meeleavaldused, boikott, õiguslikud sammud) ning nendest tulenevad implikatsioonid institutsioonile. Sihtgrupile suunatud teabe uuendamisel mängib olulist rolli ka vastaval grupil hetkel olev teave ja nende teadmiste tase.

Põhimõtted

Organisatsioonivälise kriisikommunikatsiooni või kommunikatsioonistrateegia kindlaksmääramisel tuleks järgida mõningaid põhimõtteid.

- Institutsiooni iga suurem kriis jõuab varem või hiljem avalikkuseni. Seetõttu on otstarbekas ja vajalik avalikkust juba aegsasti informeerida. Et kriisi ja hädaolukordade halduse tajumist ühiskonnas võimalikult enda huvides mõjutada, peaks kontakt meediaga olema varajane ning läbimõeldud. Õigus ei ole sel, kes vaikib.

- Isegi kui avalikkust või väliseid osapooli kõikidest üksikasjadest ei teavitata, kehtib kriisikommunikatsiooni korral põhimõte, et kõik väljaöeldu peab ka tõele vastama.

- Tegemist peaks olema faktipõhise kommunikatsiooniga, kuid kindla piirini peaks see väljendama ka empaatiat ja sisemist kaastunnet. Suhtlus peab olukorrale vastama.

- Vältida tuleb oletusi ja spekulatsioone.

- Samuti ei tohiks negatiivsetest uudistest lihtsalt vaikida, sest tänapäeval on uudiste salajasena hoidmine võimalik ainult piiratud määral. Pooltõed, salatsemine, vagur või sunnitud taganemine tekitavad kaitseseisundi.

- Kommunikatsioon peaks olema sündmuste võltsinguteta lihtsustatud kirjeldus, sest arusaamatused tekitavad hirmu.

- Avalikkusele mõeldud teavet tuleks kohandada nii, et see ei innustaks järeletegijaid ega annaks konkurentidele võimalust sellest eelist saada.

Informatsioonikanalid

Luua tuleks keskne koht, kus kriisi korral kõik välised päringud kokku jooksevad ning kus neile nõuetekohaselt vastatakse, näiteks kriisiabitelefon. Seda võib toetada erinevate organisatsiooniüksustega, näiteks ettevõtte või asutuse kommunikatsioon, avalikud suhted või pressikeskus. Olemas peaks olema telefoni- ja faksinumber ning meiliaadress, mis tuleb sobival viisil teatavaks teha. Mõelda tuleks tasuta kriisinfoliini sisseseadmisele. Vastavalt tegevusalale, institutsiooni suurusele ja oodatavale kriisile, võib kriisisituatsiooni päringutulvaga toimetulemiseks olla mõttekas kasutada spetsialiseerunud, professionaalse teenusepakkuja teenuseid (näiteks kõnekeskus). Teenusepakkuja tuleks juba varem välja valida, lepinguliselt siduda ning kriisikommunikatsiooni läbiviimiseks välja koolitada. Keskne infopunkt lisainformatsiooni saamiseks tuleks määrata ka töötajatele ning nende lähedastele. Igasuguse keskse informatsioonipunkti korral on oluline kontrollida kõikide inimeste isikuandmeid, kes soovivad sündmuste kohta teavet saada.

Peale infopunktide tuleks ette valmistada meetmed kriisi ja selle lahendamise kohta käiva informatsiooni proaktiivseks levitamiseks. Siia hulka kuuluvad internetileheküljed, aga ka kontaktid ajakirjanikega ja pressikonverentsid. Erinevate meediaasutuste esindajad on pidevas konkurentsis. Eesmärgiks on parima loo avaldamine, mis rõhutaks inimlikku tegurit ja tekitaks emotsioone. Seepärast peaks eesmärgiks olema meediaesindajate ja kohapealse inimvoolu suunamine. Meediaesindajaid peaks kiiresti teavitama ning jooksvalt sündmuste kuluga kursis hoidma. Otsese kontakti jaoks meediaga vajatakse kontaktandmeid, mis tuleb juba varem kokku koguda ja alles hoida. Abiks on kontaktvõrgustiku loomine kohalike, regionaalsete või isegi riiklike meediakanalitega ning isiklike ja usaldusväärsete kontaktide hoidmine ajakirjanike ja erialameediaga.

Laiaulatusliku mõju võib saavutada ka kasutajasõbralike veebilehekülgedega. Ettevalmistatud ja kriisi ajal kohandatud ning üleslaetud informatsioonileheküljed võivad näiteks anda teavet hetkeolukorrast. Et kriisi korral ei oleks veebilehekülgede loomiseks spetsialiste vaja, tuleb kiireks reageerimiseks juba varem luua kriisikommunikatsiooni veebileheküljed ning paigutada need institutsiooni veebiserverile nn *Dark Sites*'idena. Kasutades spetsiaalsele sihtgrupile suunatud veebilehekülgi, näiteks töötajatele intranetis või omakestele või meediale internetis, tuleb kindlustada, et teabele saaks ligi pääseda ainult autentimise kaudu.

Abivahendid ja tehnika

Et kindlustada kiiret ja sobivat suhtlust, tuleks oodatavate situatsioonide tarvis juba varem luua mallid, formuleeringud ja tekstiosad. Kasu võib olla ka sellest, kui meediale saadetakse pressimapid, mis on individuaalsed ja olukorrale vastavad ning sisaldavad spetsiaalselt ettevalmistatud ja väljavalitud taustteavet. Kriisikommunikatsiooni korral on oluline, et kunagi ei võetaks kaitsepositsiooni.

Kriisiolukorraks vajatakse sobivaid ning toimivaid kommunikatsioonivahendeid. Kommunikatsioonivahendid, tehnika ja ruumid pressikonverentsideks tuleb hädaolukorraks valmisoleku plaani järgi ette valmistada ja sisustada.

Täpsemat informatsiooni organisatsioonivälise kriisikommunikatsiooni, eriti asutuste jaoks, leiate [BMIKK-ist].

7.4 Kriisikäsiraamat

Kriisikäsiraamat on kõikide hädaolukorra lahendamiseks vajalike (osa-)dokumentide kogum, mis koondab endas vajalikud struktuurid, teabe, meetmed ja tegevused, mis on olulised pärast hädaolukorra tekkimist ja tegevuse taaskäivitamiseks. See tuleb juba varem koos hädaolukorraks valmisoleku plaaniga koostada ning sellega ühtlustada. Kriisikäsiraamatu põhilisteks osadeks on viivitamatute meetmete plaan, kriisistaabi juhis, kriisikommunikatsiooni plaan, tööprotsesside jätkamise plaanid ja taaskäivitamise plaanid. Vastavalt institutsiooni suurusele ja keerukusele võib tegemist olla ühe või mitme dokumendiga.. Väike või keskmise suurusega organisatsioon saab kõik hädaolukorraks vajaliku informatsiooni kokku võtta ühes dokumendis. Suuremate institutsioonide korral on soovitatav jagada käsiraamat mitmeks dokumendiks. Selleks, et garanteerida, et kriisi korral tegutseksid erinevad grupid korrastatult, ja et vältida konflikte, on need dokumendid omavahel ühtlustatud. Ühtse ülesehituse ja parema käsitlemise tagamiseks tuleks kriisikäsiraamatu erinevatele osadokumentidele koostada ühine dokumendimall ja -struktuur.

Kriisikäsiraamatu eesmärgiks on võimaldada pakkuda dokumenteeritud tegutsemisviise või abi, mille toel on institutsioonil võimalik hädaolukord või kriis lahendada ja kriitilisi äriprotsesse jätkata. Kriisikäsiraamat peaks ülesehituselt olema selline, et tegevusjuhiseid oleks võimalik kiiresti ja lihtsalt leida.

Kriisikäsiraamatu ülesehitamiseks on võimalik valida mitme liigenduse vahel:

- liigendamine etappide järgi, mis kajastab hädaolukorra lahendamise ajalist kulgu,
- liigendamine vastutustasandite või rollide järgi, mis lähtuvad töötlejate ülesannetest või
- liigendamine protsesside järgi, mis lähtuvad äriprotsessidest või protsessigruppidest.

See, milline liigendus ja modulatsioon valitakse, sõltub institutsiooni suurusest ja struktuurist. Erinevaid variante on võimalik omavahel segada, seejuures tuleks aga jälgida mõningaid põhimõtteid.

- Selleks, et aktualiseerimine oleks lihtsam, tuleks pidevalt muutuv informatsioon hädaolukorra dokumentatsiooni keskses kohas kokku võtta.
- Moodulitega ülesehitus peaks kindlustama, et töötajad leiavad kiiresti nende jaoks vajaliku osa. Vajadusel on võimalik see osa neile anda.
- Selleks, et hädaolukorras oleks võimalik kõiki vajalikke meetmeid kiiresti rakendada ja et olukorrast tingitud stressisituatsioonis ükski oluline ülesanne ei ununeks, tuleb jälgida, et hädaolukorra dokumentatsioon oleks koostatud täpselt ja aktuaalselt.

Näite hädaolukorra käsiraamatu sisukorra kohta leiate lisast C. Seejuures tuleb aga jälgida, et hädaolukorra plaan on koostatud vastavalt iga institutsiooni organisatoorsetele struktuuridele ja nõuetele. Koostamisel lähtutakse äriprotsesside jätkamisest ning seetõttu ei ole võimalik üldkehtivat malli luua. Näide on ainult illustreeriva iseloomuga.

7.4.1 Kiirmeetmete plaan

Hädaolukorraga toimetuleku esimeseks sammuks on isikute turvalisuse kindlustamine. Seepärast tuleb kõik erakorralised meetmed, näiteks inimeste päästmine või evakueerimine, koondada ühte vastavasse plaani.

7.4.2 Kriisistaabi juhised

Kriisistaabi juhistes, hädaolukordade halduse juhistes või hädaolukordade halduse käsiraamatus on strateegiliseks ja taktikaliseks tegutsemiseks kindlaks määratud igat sorti kriisi eesmärgiasetus, põhimõtted ja raamtingimused. Kriisistaabi juhiseid rakendatakse enamjaolt nendel juhtudel, kus kriisi ainulaadsuse ja ettenägematuse tõttu ei ole selle jaoks tegevuskava. Siia hulka kuuluvad eelkõige kriisid, mis ei tulene kahjujuhtumitest ega mõjuta äritegevuse jätkamist. Seega on sihtgrupiks üleinstitutsioonilise hädaolukordade halduse kriisistaap. Sellest tingituna tuleks see osaplaan välja töötada üleinstitutsioonilise hädaolukordade halduse raames või sellega vähemalt ühtlustada.

Hädaolukorra ja kriisi lahendamiseks nii, nagu seda käesolevas dokumendis kirjeldatud on, pakutakse kriisistaabi juhistes muuhulgas otsustusabi nii olukorra hindamiseks kui ka sobivaid plaane ja valikuvõimalusi äritegevuse jätkamiseks. Seejuures on oluline säilitada erinevate huvigruppide nõudmised. Kriisistaabi juhised sisaldavad veel põhilist teavet ülesehituskorralduse (rollid, ülesanded ja õigused), tegevuse organiseerimise ja kontaktisikute kohta, kes omavad informatsiooni kriisi lahendamisel olulise tähtsusega isikute ja firmade kohta.

7.4.3 Kriisikommunikatsiooni plaan

Kriisikommunikatsiooni plaanis on kindlaks määratud, kuidas sisene või väline side kriisi korral toimuma peaks (vt ptk 7.3). Siia alla kuulub suhtlus töötajate ning nende perekondadega, tähtsaimate huvigruppidega ja eelkõige avalikkusega ja meediaasutustega. Kriisikommunikatsiooni plaanis on vaja muuhulgas kindlaks määratud, kes tohib millise informatsiooni kellele edastada ning millisel viisil seda teha tohib. Kriiskommunikatsiooni plaan võib olla osa kriisistaabi juhisest.

7.4.4 Tööprotsesside jätkamise plaan

Tööprotsesside jätkamise plaaniga võetakse pärast kahjujuhtumit protsessitasandil kokku institutsiooni reaktsioon äritegevuse katkemisele. Eesmärgiks on situatsiooni analüüsimine ja kriitiliste äriprotsesside viivitamatuks taaskäivitamiseks sobivate strateegiate väljatöötamine. Praktika on näidanud, et iga loogilise organisatsiooniüksuse jaoks tuleks luua tööprotsesside jätkamise plaan. Tööprotsesside jätkamise plaanide eesmärgiks on pakkuda dokumenteeritud tegutsemisviisi, mille abil on võimalik kriitilisi äriprotsesse varem kindlaks määratud taaskäivitusaegade piires jätkata. Nad sisaldavad hädakäituse kirjeldust, olgu see siis algses või varuasukohas, tavastsenaariumis või vähendatud jõudlusega alternatiivprotsessi korral.

Organisatsiooniüksuste tööprotsesside jätkamise plaanid tuleb konsolideerida ning ajaliselt, personaalselt ja sisuliselt omavahel ühtlustada. Koos moodustavad nad täieliku tööprotsesside jätkamise plaani.

Tööprotsesside jätkamise plaan peaks sisaldama vähemalt järgmiseid punkte:

- kehtivusala,
- jätkustrateegia ja tegevusvariandid protsesside erinevate kahjustsenaariumite jaoks,
- loend vastutavate isikutega,
- hädaolukorrameeskondade loend koos kontaktinformatsiooniga,
- plaani aktiveerimise ja desaktiveerimise kriteeriumid,
- meeskondade alarmeerimine ja neile olukorra laiendamine,
- ülevaade äriprotsesside taaskäivitamise nõuetest,
- protsesside prioriteetide määramine ja
- juhised järeltööde koordineerimiseks.

Üksikute protsesside jaoks peaks tööprotsesside jätkamise plaan sisaldama vähemalt järgmist informatsiooni:

- meetmed, kuidas äritegevust võimalikult kiiresti jätkata,

- hädaolukorrarežiimi protsesside kirjeldused või erinevad alternatiivid (näiteks institutsioonisiseste varuressursside kasutamine, alternatiivprotsessi käivitamine) koos vajadusel vajaminevate abivahenditega,

- rollikirjeldused,

- meetmed tavaolukorra taastamiseks ja

- meetmed hilisemaks tegevuseks.

Äriprotsessid tuleb järjestada vastavalt nende prioriteedile. Plaanides kirjeldatud meetodid ja meetmed peaksid suutma tagada tööprotsesside mõjuanalüüsi käigus kriitiliste äriprotsesside jätkamiseks määratud jõudlusnõuded.

Näite tööprotsessi jätkamise plaani sisukorra kohta leiate lisast D.

7.4.5 Taaskäivitamise plaan

Taaskäivitamise plaanid sisaldavad spetsiaalseid toimimisviise ja vajalikku informatsiooni ressursside taastamiseks ja taaskäivitamiseks. Nad täiustavad seega äritegevuse jätkamise plaane ning toimivad hädaolukorrameeskondade töö alusplaanina.

Taaskäivitamise plaanid sisaldavad teavet nii üksikute ressursside kohta kui ka laiaulatuslikumaid plaane, mis hõlmavad mitme süsteemi katkemist korraga. Sellekohane näide on andmekeskuse rivist väljalangemine. Vastav laiaulatuslik taaskäivitusplaan sisaldab üleminekut varuandmekeskusele ja selle töö alustamist.

Taaskäivituse plaanid peaksid sisaldama ülevaadet ressursside prioriteetidest ning seega ka taaskäivituse järjekorda. Erinevate ressursside kohta peaks muuhulgas koguma järgmist teavet:

- kriitilisus,

- taaskäivitusaeg ja vajadusel erilised tähtajad,

- liidesed ja sõltuvad ressursid,

- lühikirjeldus,

- meetmed vigade kõrvaldamiseks, taaskäivitus, taastamine, hädaolukorrarežiim ja üleminek tavarežiimile ning

- tugiisikud, näiteks äriprotsesside spetsialist.

8 Testid ja õppused

Kindlustamaks hädaolukorra ennetamise planeerimise ja hädaolukorra ja kriiside lahendamise sobivust, tõhusust ning aktuaalsust, tuleb ennetavaid meetmeid, organisatoorseid struktuure ja erinevaid plaane testide ja õppuste abil regulaarselt kontrollida.

Testide ja õppustega kontrollitakse kontseptsiooni aluseks olevaid oletusi. Nende käigus kontrollitakse üksikute meetmete või meetmekogude korrektset realiseerimist ning tehnika toimimist. Õppused näitavad, kas hädaolukorra dokumentatsioon on kasutuskõlblik ja kas osalejad suudavad hädaolukorras neile määratud ülesandeid täita.

Õppustega harjutatakse plaanides kirjeldatut, luuakse rutiinne tegevus ja kindlustatakse lahenduste tõhus toimimine. Nendega parandatakse nii töötajate reaktsioonikiirust kui ka tegutsemiskindlust. Kuna inimesed kalduvad kriisisituatsioonide sellest tuleneva stressi tõttu mõtlematult ja kiirustades, aga eelkõige valesti ja irratsionaalselt reageerima, ei tohiks nimetatud õppuste eesmärke alahinnata.

Testid ja õppused on seotud kulutustega. Hindamaks testide ja õppuste jaoks tehtavaid investeeringuid, on vajalik asjakohane planeerimine. Sellest lähtuvalt tuleks koostada õppuste plaan. Planeerimisel peaks arvestama erinevate testide ja õppuste liikidega. Mõningaid näiteid on kirjeldatud järgmistes alapeatükkides. Testide ja õppuste liigid sõltuvad institutsiooni tüübist, suurusest ning olemasolevast keskkonnast ja seega tuleb need eraldi valida.

8.1 Testide ja õppuste liigid

Allpool kirjeldatakse mõningaid testide ja harjutuste liike. Need ulatuvad lihtsatest üksikmeetmete kontrollidest kuni keerukate õppusteni. Lihtsaid kontrolle nimetatakse käesolevas dokumendis tihtipeale testideks ning keerukaid kontrolle, mis sisaldavad stsenaariumit, nimetatakse õppusteks. Mõistete kindel piiritlemine ei ole siinkohal võimalik. Paljud väited kehtivad mõlema kontrolliliigi kohta.

Tehniliste ettevaatusabinõude test

Tehniliste lahenduste sobivuse ja funktsionaalsuse kontrollimiseks tuleb neid testida. Siia alla kuuluvad vooluvarustuse redundantne paigaldamine, andmete taastamine varukoopiatega, klastrite kindlustamine rivist väljalangemise vastu, kasutatav teavitustehnika, tehniline infrastruktuur või üksikud IT-komponendid. Üksikute komponentide koostööd ja funktsiooni tuleks regulaarselt kontrollida. Seda tuleks teha ka lähtuvalt juhtumist, näiteks süsteemi või vastava süsteemikeskkonna suuremate muutuste korral.

Funktsioonitest

Selle õppusega kontrollitakse hädaolukorrakäsiraamatu erinevates osaplaanides kindlaks määratud protseduuride, osaprotsesside ja süsteemigruppide funktsionaalsust. Seejuures kontrollitakse erinevate komponentide ja meetmete kulgu, aga ka kokkumängu ja sõltuvusi. Siia hulka kuuluvad taaskäivitamise plaanid, taastamise plaanid, ning hädaolukorra plaanid kiirmeetmetele (näiteks hoone evakueerimine tulekahjuhäire korral).

Plaani eelvaade

Plaani eelvaate eesmärgiks on hädaolukordade ja kriiside lahendamise plaanide kontrollimine. Selle testiliigi korral vaatlevad osalejad plaane teoreetiliselt ning kontrollivad, kas nende sisu ja eeldused on loogilised. Seejuures hinnatakse selgelt kirjeldatud sisu funktsionaalsust.

Plaaniarutlus

Plaaniarutlust kasutatakse probleemide ja stsenaariumite läbimõtlemiseks (*Table Top Exercise*). Selles harjutuse liigis antakse ette kindel stsenaarium, mis mängitakse teoreetiliselt läbi. Seda testiliiki on lihtne realiseerida ning see sobib plaani esmaseks kinnitamiseks. Nõnda on võimalik avastada erinevusi ja arusaamatusi enne kulukamate ja töömahukamate tegevuste käsilevõtmist. Hädaolukordade halduse loomise etapis tuleks seda kontrollimisviisi tihedamini korrata.

Staabiõppused

Plaani arutelude eriliseks vormiks on staabiõppused, mille käigus õpitakse kriisistaabi koostööd.

Laiendatud staabiõppused

Veel üheks plaaniarutelude eriliseks vormiks on laiendatud staabiõppused, mis kujutavad endast staabiõppuste täiendatud versiooni. Need on vajalikud selleks, et peale kriisistaabi koostöö harjutada ning kontrollida veel lisaks kostööd kriisistaabi ja operatiivüksuste vahel. Reeglina viiakse staabilähedastes struktuurides õppusi läbi praktiliselt, samas aga simuleeritakse operatiivset realiseerimist teoreetiliselt.

Kommunikatsiooni- ja alarmeerimisõppused

Hädaolukorra ja kriisi lahendamise nõrgaks kohaks on kriisistaabi ja teiste vastutavate isikute teavitamine ja hoiatamine. Seetõttu tuleb teavitamise, eskalatsiooni ja alarmeerimise meetmeid regulaarselt kontrollida. See test hõlmab nii kommunikatsioonivahendite lihtsat kontrollimist kui ka kriisistaabi kogunemist kriisistaabiruumi. Õppuse käigus kontrollitakse plaanides märgitud vastutavaid isikuid ja telefoninumbreid, meetodeid, eskalatsioonistrateegiaid, isikute kättesaadavust ning asetäitjate regulatsiooni. Kontrollitakse, kas olemasolevad plaanid on aktuaalsed, arusaadavad ja käepärased, kas kasutatavad meetodid on praktilised ning kas kasutatavad tehnoloogiad (näiteks alarmeerimissüsteemid, hädaolukorra telefon, SMS, piipar, raadio- ja satelliitkommunikatsioonisüsteemid) on töökorras, tõhusad ja sobivad.

Stsenaariumite simulatsioon

Reaalsuslähedase simulatsiooni kaudu testitakse hädaolukorrastsenaariumite ja -juhtumite lahendamiseks kindlaks määratud protseduuride ja meetmete asjakohasust, sobivust ja funktsionaalsust. Seejuures katsetatakse nii alarmeerimist, eskalatsiooni, hädaolukorra lahendamise organisatsiooni, kriisistaabi tööd ja kõikide seotud osapoolte koostööd. Selliseid õppuseid võib korraldada funktsiooni- või osakonnaõppustena või hilisemas etapis üleosakonnalise õppusena.

Täisõppus

Simulatsiooni kõige kulukam ja töömahukam liik on täissimulatsioon. Vastavalt stsenaariumile tuleb kaasata ka väliseid osapooli, näiteks tuletõrje, abiorganisatsioonid, ametkonnad jne. Seda õppuse liiki saab kasutada ning peaks kasutama alles edasijõudnud etapis.

Täisõppus lähtub reaalsusest ning hõlmab kõiki üksusi alustades juhatusest ja lõpetades üksiku töötajaga. Ettevalmistuse, läbiviimise ja järelanalüüsi mahtu ei tohiks alahinnata. Vaatamata sellele ei tohiks sellest loobuda kõrgete nõudmiste tõttu, mis institutsioonis hädaolukordade haldusele esitatakse. Neid tuleks läbi viia regulaarselt pikemate ajaperioodide tagant.

Õppuseliikide võrdlus

Teste ja õppusi saab eristada erinevate kriteeriumite alusel: tüübi või sihtgrupi, ulatuslikkuse ja töömahu järgi. Otsustamine võib põhineda arutelul või olla suunatud tegevusele. Sihtgruppide juures saab eristada kolme põhilist vastutusala: strateegiline, taktikaline ja operatiivne. Taktikalise tasandi õppustega kontrollitakse koordineerimist, erinevate osakondade koostööd ja tegutsemist olukorra väljaselgitamisel ja hindamisel. Operatiivsel tasandil on keskpunktis hädaolukorra lahendamiseks tehtavad tegevused ja tööd (vt tabel 18).

Õppuse liik	Sihtgrupp			Kulg		Kulu/ maht
	strateegiline	taktikaline	operatiivne	arutelul põhinev	tegevusel põhinev	madal/keskmine / kõrge/ väga kõrge
Tehniliste ennetavate meetmete test			**X**		**X**	madal
Funktsioonitest			**X**		**X**	keskmine
Plaani eelvaade		**X**	**X**	**X**		madal
Plaani kirjeldus		X	**X**	**X**		madal keskmine
Staabiõppus	**X**	X		**X**		madal keskmine
Laiendatud staabiõppused	**X**	X	**X**	**X**	**X**	keskmiselt kõrge
Kommunikatsiooni- ja alarmeerimisõppused		**X**	**X**		**X**	madal
Stsenaariumite simulatsioon		**X**	**X**		**X**	kõrge
Täisõppus	X	**X**	**X**		**X**	väga kõrge

Tabel 18. Õppuste liigid

8.2 Dokumendid

Õppuste ja testide planeerimisel ja läbiviimisel on abi erinevate dokumentide loomisest. Nende hulka kuuluvad õppuse kontseptsioon, õppuse plaan ja õppuse protokoll.

8.2.1 Õppuste käsiraamat

Kõigi institutsiooni hädaolukordade halduse testide ja õppuste kohta kehtib põhimõte, et nad peavad kulgema planeeritult ja ettevalmistatult. Selleks, et hoida tavarežiimi tõrkeid nii harvadena kui võimalik, tuleb koos institutsiooni juhtkonnaga kindlaks määrata kõikidele testidele ja õppustele kehtivad strateegilised otsused, põhimõttelised määrused, raamtingimused ja kokkulepped. Need võetakse õppuste käsiraamatus kokku ja nii moodustavad nad aluse üldiste ja üksikute õppuste planeerimisele.

Õppuste käsiraamat peaks muuhulgas vastama järgmistele küsimustele.

- Milline on testide ja õppuste strateegiline tähendus institutsioonile?

- Millised on eesmärgid, mida testide ja õppustega saavutada tahetakse?

- Milline on testide ja õppuste väärtus?

- Milliseid testide liike institutsioonis eristatakse? Millised pingutused ja kulutused on üksikute liikidega seotud?

- Mis on üksikute õppuste liikide eesmärgid institutsioonis?

- Kui palju teste ja õppuseid tuleks läbi viia? Kas õppuste sagedusele kehtivad seaduslikud või reguleerivad nõudeid?

- Milliseid rolle testide ja õppuste läbiviimisel eristatakse? Millised on nende ülesanded, õigused ja vastutused?

- Milliseid alasid tuleks testida? Osalejate ning töötajate teadmisi ja võimeid, hädaolukordade halduse tegevust, mehhanisme ja kasutatavat tehnoloogiat, hädaolukorra dokumentatsiooni, kesksete ressursside valmisolekut, meetmeplaane jne?

- Milliseid õppuste meetodeid kasutatakse (näiteks etteteatamisega, etteteatamiseta)?

- Kuidas tuleb määrata õppuste ja igapäevatöö eraldatus? Kui õppuste mõju ei ole võimalik täiesti vältida, siis millisel määral võib õppus institutsiooni igapäevategevust mõjutada?

- Kuidas tuleb teste ja õppuseid dokumenteerida? Millise täpsusega?

- Kuidas tuleb õppuse tulemusi analüüsida?

Õppuste käsiraamat sisaldab peale strateegiliste põhimõtete ka vahendeid, mis on abiks detailse plaani koostamisel, õppuste ja testide läbiviimisel ning sellele järgneval analüüsil. Siia alla kuuluvad nt mallid kutsete jaoks, teavitused, protokollid või küsimustikud analüüsi läbiviimiseks. Dokumendid tuleb konkreetse õppuse jaoks kohandada ja täita.

8.2.2 Õppuste plaan

Ei ole otstarbekas jälgida ainult üht läbiviidavat õppust, vaid rida üksteisega ühtlustatud teste ja õppusi, mis kõik kokku moodustavad terviku ja katavad kõik institutsiooni hädaolukorra plaani osad, mida on vaja harjutada. Seega määratakse õppuste plaanis mitme aasta õppuste ajad, nende järjekord ning plaanitud õppuste ja testide umbkaudsed andmed. Seejuures tuleks planeerida kõigi testide ja õppuste liigid, alustades lihtsatest süsteemitestidest ja lõpetades vähemalt stsenaariumite simulatsiooniga. Muudatuste halduse (*Change Management*) raames ei piisa ainult hädaolukorraks valmisoleku meetmete testimisest.

Testide ja õppuste läbiviimiskuupäevade kindlaksmääramisel tuleb arvestada teatud tingimustega nagu näiteks puhkuste aegadega, mil töötajad ei ole kättesaadavad, või institutsiooni ja äriprotsesside jaoks oluliste kuupäevadega. Teste ja õppusi on mõttekas läbi viia lihtsamatest keerukamateni. Teste, mis ei vaja suuremat ettevalmistust, tuleks tihedamini läbi viia. Õppuste sagedus ja maht peaksid lähtuma vastava organisatsiooniüksuse ohustatusest. Soovitatav on riskidest lähtuv tegutsemine. Mida kriitilisem on protsess või süsteem äritegevuse jätkamisele, seda tihedamini tuleks hädaolukorraks valmisoleku meetmeid ja plaane testida.

Testide ja lihtsate õppuste läbiviimisel on kasulik igaaastane rütm. Igal aastal tuleks läbi viia vähemalt üks õppus, näiteks hoone evakueerimine. Institutsioonid, kelle tegevusprotsessidel on kõrge kättesaadavuse nõue, peaksid laiaulatuslikke täisõppusi, nagu töö üle viimine varuasukohta ja hädaolukorra töökohtade funktsioonitest, viima läbi iga 2 kuni 3 aastat tagant. Sõltuvalt institutsiooni tegevusvaldkonnast tuleb läbiviimisel jälgida seaduslikke või reguleerivaid nõudeid, õppuste tüüpi ja arvu.

Õppuste plaanis määratakse iga testi ja õppuse jaoks kindlaks plaanitud stsenaarium, õppuse liik, eesmärk, kas etteteatamisega või etteteatamiseta, plaanitud osavõtjad (rollid), aeg ja eeldatav kestvus. Samuti peaks andma umbkaudse hinnangu vajaminevale personalile, materjalile ja rahalistele ressurssidele.

Plaan tuleks ühtlustada nii personaliosakonnaga kui ka juhatusega.

8.2.3 Testide ja õppuste kontseptsioon

Iga testi ja iga õppuse jaoks tuleb välja töötada vastav kontseptsioon, mis sisaldab läbiviimise detailset planeeringut. Testi kontseptsioon kirjeldab, milliste meetoditega süsteemi kontrollida, milliseid tööriistu (*Tool*) kasutatakse ning millised on etteantud raamtingimused. Õppuse kontseptsioonis kirjeldatakse muuhulgas osavõtjate hulka, iga osavõtja rolli õppusel, ajalisi piire ning tingimusi õppuse katkestamiseks. Seega sisaldab see vähemalt järgmiseid andmeid:

- õppuse nimi,
- kuupäev, aeg ja oletatav kestvus,
- õppuse koht,
- õppuse liik,
- eesmärgid,
- õppuse juhatajad,
- osavõtjad, vaatlejad, dokumenteerijad,
- juhiste jagamine osavõtjatele ja
- stsenaarium.

Õppuse kontseptsiooni loomine peaks olema kaheastmeline. Esmalt koostatakse üldine kontseptsioon, mis esitatakse juhtkonnale kinnitamiseks. Alles pärast seda koostatakse detailne kontseptsioon. Pikema kestvusega õppuste, näiteks täisõppuste, korral tuleks jälgida veel teisigi punkte. Siia alla kuuluvad näiteks ettevalmistused õppusel osalejate isikute turvalisuse tagamiseks või toitlustamine.

Õppuste stsenaarium

Laiaulatusliku stsenaariumi korral tuleb luua õppuste stsenaarium. Selles kirjeldatakse nii täpselt kui võimalik lähteolukorda, õppuse konkreetseid ajalisi piire, varem määratud sündmusi ja nende järjekorda. Samuti tuleb kindlaks määrata, kelle kaudu ja kuidas vastav teave osavõtjateni jõuab. Stsenaarium toetab õppuse tegevuse arendamisel õppuse jälgimist.

Õppuse stsenaariumi väljatöötamisel kasutatakse enamasti stsenaariumitehnikat. Seejuures kujutatakse situatsiooni reaalseid arenguvõimalusi lähtuvalt institutsiooni võimalikest kahjujuhtumitest. Harjumuse vältimiseks ja töötajate pidevaks motiveerimiseks peaks iga õppuse ja seega ka iga õppuse stsenaariumi eraldi kujundama.

Lähteolukord dokumenteeritakse nn „sinisel kihil". Seda kasutatakse õppuse alguses ning sellega antakse osalejatele hetkeolukorra kohta teavet. See sisaldab tavaolukorra kirjeldust, kahjujuhtumi teket, kogu vajalikku informatsiooni hetkeolukorra kohta, ja lõppeb „ülesandega", mis vastab reaalsele häirele. Mõiste „sinine kiht" tuleneb sellest, et tavaliselt märgitakse kogu õppuse lähtesituatsiooniga seotud kirjalik informatsioon sinisele paberile, et seda ei oleks võimalik teiste dokumentidega segamini ajada.

Üks õppuse stsenaariumi kujutamise võimalusi on tabel. Selles saab vajadusel eraldi dokumenteerida tegevuse numbri, ajahetke, sündmuste lühikirjelduse, testi eesmärgi, oodatavad reaktsioonid, osalised, kasutatud abivahendid või tööriistad (nt tabel 19).

Õppus: XYZ											
Nr	Reaalne aeg	egStsenaariumi	Märksõna	**Tegevus**	**Eesmärk / oodatav reaktsioon**	Algataja	**Osalejad**				**Abivahendid/ tööriistad/ alustamise liik**
							A	**B**	C		
1											
2	10:10		Teade LZ-le	(Kirjeldus taustainformatsiooniga)	Teate kontrollimine, eskalatsioo	Hr Jansen		**X**	**X**		Mobiil
J											

Tabel 19. Näide õppuse stsenaariumi kohta

8. 2. 4 Testide ja õppuste protokoll

Testide ja õppuste läbiviimine tuleb nn testide ja õppuste protokollides dokumenteerida. Protokollis märgitakse, millisel tegevusplaanil test või õppus põhineb, milline oli osalejate tegevus, milliste meetodite järgi tegutseti, milliseid tööriistu ja konfiguratsioone kasutati ning millised tulemused saavutati. Eelkõige peaks dokumenteerima testi või õppuse plaanis kindlaks määratud eesmärkidega seotud probleeme või kõrvalekaldeid. Testi või õppuse protokoll moodustab aluse neile järgnevale analüüsile, nõrkade kohtade väljaselgitamisele ja parandusettepanekute tegemisele.

8.3 Testide ja õppuste läbiviimine

8.3.1 Põhimõtted

Testide ja õppuste läbiviimisel tuleb arvestada mõningate põhimõtetega. Näiteks ei tohiks need segada tavarežiimi. Läbiviimise ajahetke valimisel tuleks seega arvestada, et õppus võib otseselt mõjutada institutsiooni põhitegevust. Testitavad süsteemid ei ole testi ajal tavakäituseks kasutatavad või on seda ainult vähendatud jõudlusega. Selleks, et hoida testi mõju jooksvatele tegevusprotsessidele võimalikult väiksena, on teste ja õppusi soovitatav läbi viia väljaspool tavapäraseid tööaegu.

Õppusesse kaasatud töötajad peavad õppuste ajal oma igapäevase töö pooleli jätma. Tehtud töötunnid tuleb tasustada. Kui teste ja õppusi viiakse läbi väljaspool regulaarseid tööaegu, tuleb personaliosakonnaga sõlmida vastavad kokkulepped.

Tuleb planeerida meetmeid, mis kindlustavad, et testimine jääks läbiviijate kontrolli alla ega tekitaks ise ühtegi tõrget. Õppuse ootamatute tõrgete korral tuleb kindlaks määrata katkestuskriteeriumid ja plaanida varulahendus (*fallback solution*), millega saaks tavalise äritegevuse võimalikult kiiresti taastada. Õppuse katkestuskriteeriumid võivad olla nt kindla ajavahemiku ületamine või arusaam, et realiseeritavad meetmed ei anna soovitavat edu.

8.3.2 Rollid

Nii õppuse planeerimisel, ettevalmistamisel kui ka läbiviimisel on vaja teha ulatuslike töid. Seepärast tuleb õppuse ettevalmistamiseks ja läbiviimiseks kindlaks määrata vastavad isikud ning nende ülesanded ja õigused.

Õppuste koostaja

Õppuste ettevalmistamiseks tuleks määrata õppuste autor. Tema ülesannete hulka kuulub õppuste plaani koostamine ja üksikute õppuste kontseptsiooni kindlaksmääramine, stsenaariumite kindlaksmääramine, osalejate väljavalimine ja õppuste jaoks sobiva keskkonna loomine. Neid ülesandeid ei tohiks alahinnata – need nõuavad vastavalt õppuse liigile rohkem või vähem jõupingutusi. Õppuste koostaja peaks hästi tundma hädaolukorraks valmisoleku plaani, aga ka hädaolukorra-, taaskäivitus- ja taastamisplaani. Seda rolli saavad täita ka hädaolukorra spetsialist või kriisistaabi juht.

Ettevalmistusmeeskond

Õppuse kontseptsioonide ja stsenaariumite loomiseks ja töötlemiseks vajab õppuste koostaja ettevalmistusmeeskonna abi. Ettevalmistusmeeskonda võivad kuuluda osakondade juhatajad või protsesside eest vastutavad isikud, kes saavad siinkohal kasutada oma erialateadmisi.

Õppuste juht / jälgija

Õppuste läbiviimisel on keskne roll õppuste juhil või jälgijal. Tema ülesannete hulka kuulub õppuste avamine, üksikute tegevuste koordineerimine, otsuste tegemine alternatiivtegevuste või plaanist kõrvalekaldumiste kohta ning õppuste ametlik lõpetamine.

Tuumikmeeskond

Õppuste juhti toetab juhtgrupp. Nende ülesanneteks on asjakohane nõustamine, õppusest osavõtjate küsimustele vastamine või õppusstseenis üksikute tegevuste algatamine. Lisaks kuuluvad tuumikmeeskonda protokollijad, õppuste autor, hädaolukorra spetsialist ja teatud juhul ka vaatlejad.

Dokumenteerija

Dokumenteerija ülesandeks on õppuse kulgemise detailne dokumenteerimine. Sõltuvalt õppuse mahust, asukohtade arvust, esindatud huvigruppidest ja teistest teguritest võib olla vajalik ka mitme protokollija olemasolu. Mitmel protokollijal on võimalus olukorda osaliselt erinevatest vaatepunktidest näha ja dokumenteerida.

Vaatlejad

Protokolliandmete kõrval võib õppustele lubada ka vaatlejaid. Vaatlejate hulka võivad kuuluda näiteks revisjoniliikmed, aga ka teiste osakondade liikmed, välised eksperdid või ametkondade ning abiorganisatsioonide esindajad. Õppuse läbiviimisel käituvad nad neutraalselt ega sekku tegevusse. Samas tuleks ka see grupp kaasata õppuste analüüsi, võttes arvesse nende tähelepanekuid ja hinnanguid.

Osalejad

Osalejate hulka võivad kuuluda protsesside eest vastutavad isikud, organisatsiooniüksuste eest vastutavad isikud, töötajate ja juhtkonna esindajad, aga ka kliendid, teenusepakkujad, tarnijad või teised välised osapooled. Niikaua, kui hädaolukordade haldus on veel planeerimisetapis, tuleks väliste osapoolte kaasamisest loobuda.

8.3.3 Õppuste protsess

Õppuste läbiviimise võib üldjoontes jagada nelja etappi.

Plaanimine ja lubamine

Testide ja õppuste läbiviimist tuleb planeerida nagu projekti. Siia alla kuuluvad aja ja personali planeerimine, hõlmates kogu õppuse perioodi alates kontseptsioonist ja lõpetades järeltööga. Stsenaarium töötatakse välja ja õppuse läbiviimiseks vajalikud dokumendid koostatakse.

Õppuste kontseptsiooni peab kinnitama ja lubama institutsiooni juhatus. Seda võib teha pärast planeerimist, kuid samas võib kulukate väärplaneeringute vältimiseks lasta õppuste plaani umbkaudse versiooni juba varem kinnitada.

Ettevalmistus

Otseses ettevalmistusetapis luuakse õppuse läbiviimiseks vastavad eeldused. Siia alla kuulub näiteks keskkonna loomine ja võimalike ettevaatusabinõude või turvameetmete sisseseadmine, näiteks andmevarundus ja varusüsteemide sisseseadmine või päästeteenistuste, ametkondade ja kohaliku pressi informeerimine. Nõnda välditakse arusaamatuste ja valehäirete tekkimist. Kehtib põhimõte, et õppuste ressursid peavad vastama taaskäivitamise plaanidele.

Vastavalt osalejate teadmistele on neid soovitatav teavitada õppuse läbiviimisest, mõttest, meetmetest ja tegevuse kulgemisest. Õppusega samal ajal toimub infotund, kus selgitatakse aktuaalseid rolle, tutvustatakse ajakava ning antakse teavet kontaktisikute ja telefoninumbrite kohta. Sõltuvalt õppuste liigist ja eesmärgist ei ole kõigi osaliste täielik teavitamine vajalik. Isikud, kes juba varem saavad teavet tegevuse kulgemise kohta, tuleb kindlaks määrata õppuse planeerimisel. Samuti tuleb kindlaks määrata, millal nad teavet saavad ja milline see teave on.

Läbiviimine

Õppusega alustatakse juba varem kindlaks määratud ajahetkel õppuse juhi märguande peale. Õppuste juht koordineerib tegevust ja otsustab, kas ja kuidas plaanist kõrvale kalduda tohib.

Õppuste juht peaks osalisi juhendama, et olukord kaootiliseks ei muutuks, aga samas peaks ta neile jätma võimalusi loovalt tegutseda. Selleks, et hoida õppuseid pidevas arengus, algatavad vastavad osalejad õppuste stsenaariumis määratud tegevused.

Dokumenteerimist juhivad määratud protokollijad. Protokollis peaks õppuse juht dokumenteerima õppuse kulgemise, saavutatud eesmärgid, ning raskused ülesannete lahendamisel. Sissekanne peaks sisaldama tähelepanekuid, kuupäeva ja kellaaega, märkusi ning vaatleja nime. Õppuste protokoll on hilisema analüüsi aluseks. Protokoll on sisesele või välisele revisjonile tõendiks õppuste läbiviimise kohta.

Õppuste juht peaks iga õppuse ametlikult lõpetama. Õppuste jaoks loodud keskkond tuleb pärast õppusi viia tagasi tavaolekusse. Erinevates kohtades läbi viidud õppuste korral tuleb dokumendid ühte kohta kokku koguda.

Pärast õppuse lõppu tuleks kõigi osalenutega viia läbi lühike koosolek. Koosoleku sisuks on õppuse kokkuvõtmine ja võimaliku eelhinnangu andmine.

Järelanalüüs

Õppuseid peaks analüüsima varem kindlaksmääratud inimeste koosolekul. Analüüsi käigus võrreldakse saavutatud tulemusi seatud eesmärkidega ning dokumentatsiooni alusel analüüsitakse sündmuste kulgemise probleemkohti. Eesmärgiks on nii hädaolukorraks valmisoleku, hädaolukorra lahendamise, kui ka õppuste läbiviimise täiustamispotentsiaali tuvastamine. Aluseks on õppuse protokoll, aga ka õppusel osalejate ning vaatlejate hinnangud.

Õppuse analüüs tuleb dokumenteerida. Õppuse juht koostab läbiviidud õppuse ja tulemuste kohta lõpparuande ning esitab selle juhatusele.

Kindlaks tuleb määrata vastutused ja meetmed puuduste kõrvaldamiseks ning samuti tähtajad antud meetmete rakendamiseks. Hädaolukorra spetsialist kontrollib meetmete rakendamist. Kasutusele võetud meetmete tõhusust tuleks kontrollida hiljemalt järgmiste õppuste ajal.

9 Hädaolukordade halduse toimimise tagamine ja pidev täiendamine

Hädaolukordade halduse toimimise tagamiseks ja pidevaks täiendamiseks ei tule ainult ettevaatusabinõusid realiseerida ja dokumente ajakohastada, vaid ka hädaolukordade halduse protsessi enda toimimist ja tõhusust tuleb regulaarselt kontrollida. Seejuures peaks juhtkond protsesse regulaarselt kontrollima ja hindama (halduse kontroll). Kõik sündmused ja otsused tuleb arusaadavalt dokumenteerida.

9.1 Toimimise tagamine

Selleks, et saavutada hädaolukordade halduse ja hädaolukorra ennetavate meetmete efektiivsus, tuleks meetmeid pidevalt valvata, juhtida ning ajakohastada. Järelevalve võimaldab juba varakult hädaolukordade halduse täiustuspotentsiaali tuvastada. Alusena peaks iga institutsiooni jaoks välja töötama sobivad mõõtmis- ja hindamiskriteeriumid. Need mõõteväärtused tuleb regulaarselt välja selgitada ja nende väärtuste arengut tuleb jälgida. Väärtuste negatiivse arengu korral tuleks välja selgitada põhjus, määrata parandusmeetmed, nimetada läbiviimise eest vastutavad isikud ning väärtused kohandada. Tulemused tuleks aruande vormis kokku võtta ja juhtkonnale edastada. Siin kirjeldatud sammude eest vastutab hädaolukorra spetsialist.

Sobivad mõõtmis- ja hindamiskriteeriumid võiksid olla näiteks:

- läbiviidud õppuste arv (edukad/mitteedukad),
- läbiviidud testide arv (edukad/mitteedukad),
- tekkinud hädaolukordade arv (edukalt lahendatud),
- läbiviidud koolituste arv (osavõtjate arv /kestus tundides),
- kriisistaabi alarmeerimiseks vajalik aeg
- või vähendatud riskide arv võrreldes riskide koguarvuga.

Hädaolukordade halduse protsesside valve ja juhtimise kõrval mängib olulist rolli meetmete ja eelkõige dokumentide aktuaalsus. Nende aktuaalsuse säilitamiseks on oluline sisestada erinevatesse äriprotsessidesse muutuspäästikprotsessid. Päästikprotsessid tuleks aktiveerida siis, kui muudatusi tehakse

- institutsiooni strateegilises suunitluses, ärivaldkondades või huvigruppide prioriteetides,
- raamtingimustes, nt seaduslikes või muudes tingimustes,
- keskkonnas, nt muutused institutsiooni asukohas või institutsioonisisene kolimine (näiteks hädaolukorra töökohad),
- äriprotsessides,
- personalis,
- kasutatud tehnikas või
- ainult süsteemi tarkvaras, niivõrd kui see on osa hädaolukorraks valmisoleku plaanist.

Pärast seda tuleb kontrollida vastavat hädaolukordade halduse osa ja vajadusel rakendada kohandamismeetmed muudatushalduse kaudu.

9.2 Kontrollimine

Ainult hädaolukordade halduse protsesside ja hädaolukorraks valmisoleku meetmete regulaarse kontrolli kaudu on võimalik hinnata institutsiooni võimeid hädaolukordi ja kriise lahendada. Eesmärgiks on kindlustada hädaolukordade halduse funktsionaalsus, efektiivsus, sobivus ja tõhusus. Selleks otsitakse parandusvõimalusi ja vigu ning antakse soovitusi.

Hädaolukordade haldust kontroll peaks kontrollima mitmel erineval tasandil. Kõige sisemise kihi moodustab enesele antud hinnang (*Self Assessments*), mille korral hädaolukorra spetsialist ja koordinaatorid hindavad ja lasevad hinnata nende poolt etteantud määrusi, hetkel kaetud ala ja hädaolukordade halduse tõhusust ning valmisoleku taset. Seejuures kontrollitakse muuhulgas, kas meetmeid rakendatakse etteantud määruste kohaselt, kui palju etteantud meetmetest on rakendatud ja kas neid täidetakse.

Järgmiseks sammuks on sõltumatute auditite läbiviimine siseauditi poolt. Seda tehakse lähtuvalt ametiseisundi tunnustatud põhimõtetest. Siseauditeid tehakse juhatuse käsul. Siseauditite kaudu dokumenteeritakse muuhulgas ka asjaolu, et juhatus täidab oma kontrollfunktsiooni. Kontrollijad peavad olema erapooletud ja kompetentsed (vajadusel tuleb seda kontrollida). Siseauditi korral vaadeldakse erilise täpsusega sisemistest ja välistest suunistest kinnipidamist ning võrdlust standardite ja hea tava (*Best Practise, Compilance*) vahel. Samas tuleb kontrollida ka hädaolukordade halduse protsesside efektiivsust ja sobivust.

Hädaolukordade halduse siseauditit peaks planeerima vastavalt riskiorientatsiooni lähenemisele ning see tuleb institutsiooni juhatusega kooskõlastada. Kontrollimise plaaniga määratakse kindlaks kontrollide eesmärgid, liigi, mahu ja sisu ning kontrollide rollid. Revisjoni läbiviimise käigus tuleb kõik olulised tähelepanekud dokumenteerida ning hiljem järeltöötluse käigus tuleb neid analüüsida. Kontrollimismeetodina võib kasutada dokumentide kontrollimist, interviusid või ringkäike. Sündmused tuleb dokumenteerida auditi aruandes, mis sisaldab järeldusi ja tegevuskava. Revisjoni aruanne tuleb edastada hädaolukorra spetsialistile ja juhtkonnale.

Välisauditid käivitatakse väliste järelevalveorganite poolt. Välisauditite tegemiseks palgatakse ettevõtetes enamasti audiitorid või konsultatsioonifirmad. Meetodid ja tegutsemisviis vastavad rahvusvahelistele auditeerimisstandarditele, näiteks IDW (*Institut der Wirtschaftsprüfer in Deutschland*) standarditele. Asutustes viiakse välisauditid tavaliselt läbi kontrollkoja poolt.

Hädaolukordade halduse regulaarset kontrollimist tuleb planeerida, see tuleb läbi viia ja tulemused tuleb dokumenteerida. Kontrolli käigus avastatud probleemid tuleb võimalikult kiiresti kõrvaldada. Sellest lähtuvalt on hädaolukorra spetsialistil vaja välja töötada vajalikud korrigeerivad meetmed ning need teostusplaani näol dokumenteerida. Teostusplaan sisaldab ajakava, ressursside planeerimist, vastutuste määramist ning etteantud määrusi ja teostusseisu kontrolli. Hädaolukorra spetsialist vastutab ka korrigeerivate meetmete rakendamise ning vajalike ressursside sobiliku kasutamise eest.

9.3 Info liikumine ja halduse kontroll

Selleks, et institutsiooni juhtkond saaks hädaolukordade halduse protsesside juhtimisel teha õigeid otsuseid, vajab see teavet hetkeolukorra ja hädaolukordade halduse arengu kohta. Hädaolukorraks valmisoleku organisatsioon peab juhtkonnale sobival viisil haldusaruannetes edastama teavet kontrollide tulemuste ja hädaolukordade halduse protsesside olukorra kohta. Seejuures tuleks üles märkida probleemid, edukad lahendused ja parandusvõimalused. Juhtkond vaatab haldusaruande läbi, hindab olukorda ja vajadusel viib sisse korrigeerivad meetmed. See hinnang peaks sisaldama järgmiseid aspekte:

- auditite tulemused (ka teenusepakkujate ja tarnijate omad),
- testide ja õppuste tulemused,
- ettepanekud meetmete jaoks pärast hädaolukorra lahendamist,
- meetmestaatus (ennetavad meetmed, reaktiivsed meetmed),
- riskid (jääkriskid, aktsepteeritud riskid, ohud, mida pole arvesse võetud, ja nõrgad kohad),
- uued lahendused (tooted, meetodid) efektiivsuse parandamiseks (näiteks tarkvaratoega hoiatamine),
- koolitus- ja teavitusprogrammide tulemused, uued

standardid või - head tavad (hädaolukordade haldusele),

- kõik muudatused, mis võivad hädaolukordade haldust mõjutada (näiteks alltöövõtuna saadud protsessid) ja
- viimasest halduskontrollist pärinevate meetmete rakendamise seis.

Vaatamata siin nimetatud paljudele erinevatele aspektidele peaks halduskontroll olema lühike ja ülevaatlik.

Hinnangule peaks järgnema paranduse tegemine, mis siinkohal tähendab korrigeerivate meetmete elluviimist. Need võivad olla ennetavad või muuta hädaolukordade halduse protsessi osi. Siia alla kuuluvad näiteks:

- kasutada antud eelarve kohandamine,
- eesmärkide ja juhiste kohandamine,
- strateegia muutmine (üksikute ressursside või kogu strateegia jaoks),
- hädaolukorra organisatoorse ülesehituse kohandamine,
- meetmete muutmine, et oleks võimalik reageerida nii organisatsioonisisestele kui -välistele nõudmistele,
- nõudmised äriprotsessidele,
- nõudmised katkestuste vastasele kaitsele,
- reguleerivad või lepingulised nõudmised ja
- muudetud riskivalmidus.

Selleks, et juhtkonnal oleks lihtsam otsuseid teha, on soovitatav, et hädaolukorraks valmisoleku organisatsioon teeks juhtkonnale esitatavas halduskontrollis meetmete kohta juba konkreetseid ettepanekuid. Institutsiooni juhtkonna eesmärgiks peaks olema halduskontrolli põhjal hädaolukordade halduse efektiivsuse pidev tõstmine. Seetõttu tuleb analüüsi tulemused ja kindlaksmääratud meetmed dokumenteerida ja järgmise analüüsi ajal tuleb meetmete teostusastet kontrollida. Hädaolukorraks valmisoleku organisatsioon peaks kontrollima uuesti rakendatud meetmete tõhusust ja vajadusel neid veel kord parandama.

10 Hädaolukordade haldus ja väljasttellimine

Teenuste või tööprotsesside väljasttellimiseks on mitmeid põhjusi, alates soovist suunata kogu energia tuumtegevusele ja kulutusi kokku hoida kuni riskide hajutamiseni. Arengud viitavad sellele, et endiselt kasvab trend ühendada ettevõtteid ja asutusi üha komplektsemalt väljasttellitavate teenustepakkujatega ja tarnijatega – seda erinevate lepingute, liideste ja kontaktisikute kaudu. Majanduslikust vaatepunktist positiivsete argumentidega nagu kulude kokkuhoid või keskendumine tuumtegevusele kaasnevad aga ka spetsiifilised riskid tööprotsessidele ja turvalisusele, mida ei tohiks alahinnata. Iga väljasttellitav projekt on seotud mitmete turvariskidega. Lähemalt on sellest juttu IT-etalonturbe kataloogi moodulis "B 1.11 Väljasttellimine".

Hädaolukordade halduse aspektist tähendab ettevõtte põhitegevust toetavate äriprotsesside sisseostmine seda, et kasvab organisatsiooni väljastpoolt ohustatavate riskide arv. Sellega on seotud kontrolli kadumine. Lisaks on ohustatud teenusepakkujaga seotud organisatsioonisisesed tööprotsessid. Riskide vähendamiseks tuleb nii uute väljasttellitavate projektide ja tarnekokkulepete plaanimisel ning vastavate lepingute koostamisel kui ka jooksvate projektide elluviimisel silmas pidada erinevaid aspekte. Allpool puudutakse mõnda neist lühidalt.

10.1 Plaanimine ja lepingute koostamine

Väljasttellitavate projektide plaanimisel tuleks lisaks turvahaldusele silmas pidada ka hädaolukordade haldust. Oluline on eelnevalt välja selgitada, milline on plaanitava teenuse või tarnitava toote kriitilisuse aste ja millised riskid väljasttellimisega kaasnevad. Hädaolukorraspetsialist peab tagama, et lepingusse saaksid kirja pandud väljasttellitavate tööprotsesside hädaolukordade haldusele esitatavad nõuded.

Kui teenust hinnatakse kriitiliseks või väga kriitiliseks, tuleb kontrollida teenusepakkuja hädaolukordade halduse võimet ja lisada lepingusse hädaolukordade haldust puudutav klausel või lisa.

Lisaks soovitavatele teenustele tuleb põhjalikult analüüsida ja kirjeldada konkreetseid nõudeid, mis esitatakse tulenevalt tööprotsesside mõjuanalüüsist (BIA) väljasttellitavate tööprotsesside käideldavusele. Samuti tuleb detailselt kirjeldada väljasttellitava teenusepakkuja hädaolukorra- ja kriisihalduse võimet. Tuleb nõuda, et teenusepakkuja koostaks väljasttellitavate protsesside taaskäivitamise ja taastamise plaanid. Koostatud plaanide realiseerumisvõimet peab kontrollima tellija hädaolukordade haldustalitus. Olenevalt väljasttellitavatest protsessidest ning institutsiooni ja teenusepakkuja vahelisest liidetest võib olla vaja läbi viia ühiseid hädaolukorraharjutusi. Valmisolek harjutusi läbi viia ja ühiselt kulusid kanda peab olema sätestatud väljasttellimislepingutes. Lisaks ühistele harjutustele peaks teenusepakkuja suutma oma üldist hädaolukorra- ja kriisihaldamise võimet tõendada ka muude regulaarselt läbiviidavate testide ja harjutustega, seda eriti osutatavate teenuste suhtes. Kui teenusepakkuja juures läbiviidavad organisatsioonisisesed harjutused võivad kahjustada väljasttellitavaid protsesse, tuleb tellijat sellest aegsasti teavitada. Lepingus peab olema sätestatud ka koostöö tegemine hädaolukorra või kriisi ajal, aga ka mõlema poole õigused ja kohustused. Mõned olulised õigused ja kohustused oleksid näiteks järgmised.

- Selleks, et läbi viia organisatsioonisisest auditit või et seda saaks teha organisatsiooni poolt nimetatud välisaudiitor, peab tellival institutsioonil olema õigus välist teenusepakkujat kontrollida.

- On oluline kehtestada teenusepakkuja teavitamiskohustused ja neid üksikasjalikult kirjeldada. Teenusepakkuja peab tellijat teavitama näiteks muudatustest hädaolukordade halduses, hädaolukordade halduse kontseptsioonis või ka oluliste kontaktisikute vahetumisest. Ka tellija peab teenusepakkujat teavitama muudatustest, mis puudutavad väljasttellitavaid protsesse.

- Teenusepakkuja peab tellijat regulaarselt teavitama olulistest asjaoludest, nagu auditite

tulemused või hädaolukordade halduses tekkinud probleemid.

- Tellimuse täitja peab tellijale pidevalt osutatud teenuste kohta andmeid esitama (nt helpdesk'ilt) või andma tellijale õiguse teha vastavat seiret.

- Teenuse osutaja on kohustatud informeerima tellijat oma ettevõtte arengutest, mis võivad kahjustada kokkulepitud teenuse osutamist.

- Selleks, et teenuse osutaja saaks kriisi korral adekvaatselt reageerida, tuleb määratleda, kas kriisi ajal on kõige tähtsam infoturve või tööprotsesside jätkamine.

- Väljasttellimise osapoolte vahel peavad olema kindlaks määratud eskalatsiooniastmed ja -teed, et hädaolukorra korral ei tekiks viivitusi ega vääritimõistmisi.

- Teenusepakkujaga tuleb kokku leppida tema reageerimise ja kättesaamise tagamise suhtes, kaasa arvatud tema ööpäevaringse kättesaadavuse suhtes hädaolukorra korral.

- Tellijal peab hädaolukorra ja kriisi ajal olema õigus teha teenusepakkujale ettekirjutisi (mis puudutavad osutatavat teenust).

- Väljasttellimise osapooled peavad omavahel kokku leppima, millised võimalused on hädaolukorra korral teenuse osutamise jätkamiseks, ja veenduma võimaluste kasutamise tõenäolisuses.

- Lepingus peaks olema sätestatud tellija õigus lepingu rikkumise või nõuetest mitte kinnipidamise korral leping erakorraliselt üles öelda

Lepingu koostamisel tuleks üle kontrollida lõpuklauslid, muuhulgas see, mis sisaldab viidet vääramatutule jõule, et kriisi ajal ei tekiks olukorda, kus teenuse osutamine muutuks teenusepakkuja vastutuselevõtmise tõttu võimatuks.

Teenusepakkuja valikul tuleks tähelepanu pöörata sellele, et teenusepakkujal oleks ka hädaolukorra korral võimalik tellijale teenust osutada ja et tellija hädaolukordade halduse meetmed vastaksid teenusepakkuja omadele. See tähendab muuhulgas, et teenusepakkuja osutaks tellijale teenust ka asendustöökohal.

10.2 Olukorraga arvestamine kontseptsiooni loomisel

Hädaolukordade halduse loomisel ja vastavate meetmete kavandamisel tuleks tähelepanu pöörata väljasttellitavate tööprotsesside ja ka tarnijate üksikutele tööetappidele. Nendega tuleb arvestada nii tööprotsesside mõjuanalüüsi (BIA) kui ka riskianalüüsi tehes. Väljastellitavate tööprotsesside mõjuanalüüsi eesmärgiks on protsesside taaskäivitamisele ja taastamisele esitatavate nõuete kindlaksmääramine ja nende võrdlemine lepingus sätestatutega, et avastada teenuse osutamise kirjelduses võimalikke puudusi (nt maksimaalne vastuvõetav katkestusaeg, taaskäivitamisaeg, maksimaalne taastamisaeg).

Riskianalüüsis tuleb vaadelda nii väljasttellitavate ja organisatsioonisiseste tööprotsesside liideseid kui ka väljasttellitavaid tööprotsesse eraldi, et kindlaks määrata võimalikud riskid. Nii väljasttellitavad tööprotsessid ise kui ka liidesed organisatsioonisiseste protsessidega kujutavad endast võimalikke riske. Tuleb välja selgitada, millist mõju võib avaldada ühe väljasttellitava protsessi ajutine seiskumine. Selle mõju tuleks uurida aste-astmelt kuni väljasttellitava teenusepakkuja täieliku äralangemiseni. Sellele tuginedes tuleks välja arendada vastavad ettevaatusabinõud ja turvameetmed. Riskianalüüsi tegemisel ei peaks piirduma ainult tööfaasiga, st vaatlema mitte ainult jooksvaid väljasttellitavaid protsesse, vaid analüüsida tuleks ka mõne teise välise teenusepakkuja teenusena pakutavaid protsesse ja nende etappe.

Hädaolukorraplaanide koostamisel tuleb siseprotsesside ja väljastellitavate protsesside liideseid täpselt määratleda ja vastavad plaanid tuleb üksteisega ühitada. Väljasttellitava teenusepakkuja hädaolukorraprotseduurid peavad olema ühildatavad tellija omadega. Nende ühildatavus tuleb tellija ja teenusepakkuja ühiste testimiste ja harjutamiste käigus üle kontrollida.

Vastavalt võimalike kahjude suurusele nõuab hädaolukorra likvideerimine tihedat koostööd teenusepakkujatega. Seepärast peaks lepingutes olev teenuse osutamise kirjeldus sisaldama ka regulatsioone hädaolukorra eskalatsiooniks, selle likvideerimise aktiviseerumiseks ja kriisi kõrvaldamiseks. Institutsiooni enda hädaolukordade halduse kontseptsioonis peaks olema selgelt reglementeeritud, kuidas peaks toimima kriisi likvideerimisele suunatud kommunikatsioon ja kuidas on jaotatud väline kriisikommunikatsioonpädevus. Hädaolukordade haldusprotsesside ja hädaolukorraennetuse meetmete regulaarsesse kontrolli on vaja kaasata ka väljasttellitavad protsessid ja teenusepakkujad. Teenusepakkuja hädaolukorra- ja kriisihaldusvõimet võib tõendada ka tema sertifitseerimine või mõni muu sõltumatu kontroll, kuid tellija peaks jälgima, et teenusepakkuja sertifitseerimise kehtivusalas oleks ka tema tellitud tööprotsess, et teenusepakkujat loetaks projektis osalejaks ja et tööprotsesside kriitilisus oleks vastavalt lepingule astmeteks jaotatud ja teenusepakkuja hädaolukorraplaanidesse kaasatud.

Olenevalt väljasttellitavate protsesside komplekssusest ja kriitilisusest tuleks seepärast sisse seada väljasttellitavate teenuste haldus, mille eest vastutaks institutsiooni juhtkond. Lepingu mõlemad osapooled peaksid nimetama ühe vastutava kontaktisiku.

11. Tarkvaratööriistad

Hädaolukordade haldusprotsesside erinevate ülesannete ja etappidega toimetulekuks on olemas mitmesugused tarkvaratööriistad. Müügil olevad tarkvaratööriistad on ette nähtud hädaolukordade haldusprotsessi erinevate aspektidega toimetulekuks. Nende abil saab näiteks toetada tööprotsesside koostamist, läbi viia ja hinnata tööprotsesside mõjuanalüüsi (BIA), teha riskianalüüsi, koostada ja värskendada hädaolukorrakäsiraamatut, läbi viia auditeid, teste ja harjutusi ning aktiivselt hädaolukordasid likvideerida, seda alates hoiatamisest kuni protokollimiseni ja olukorra hindamiseni. Olenevalt kasutatavast tarkvarast on võimalik:

- toetada hädaolukordade halduse plaanide koostamist ja värskendamist,
- uuendada ja selgelt liigitada hädaolukordade halduse dokumente,
- juhtida automaatselt saadetava meiliteate abil olemasolevate dokumentide värskendamistsüklit,
- koostada ülevaadet kriitiliste tööprotsesside olemasolevatest plaanidest,
- luua automaatne side üksikute taaskäivitamisplaanide ja vastavate ressursside (rakendus ja süsteemid) vahel (et hädaolukorra korral oleks olemas kiire ja ühene liigitus),
- automatiseerida otsekohe rakenduv hoiatussüsteem
- protokollida kriisistaabi tegevust nõuetekohaselt.

Sobivate tarkvaratööriistade kasutamine võib hädaolukordade haldusega seotud inimeste tööd tunduvalt lihtsustada. Mõned tarkvaratooted eeldavad spetsiaalsete meetodite ja toimimismudelite kasutamist. Selle järgi saavad kasutajad orienteeruda näiteks tööprotsesside mõjuanalüüsi (BIA) või riskianalüüsi koostamisel. Vastavate küsimustike ja hinnangute andmise skeemid on ette antud ning neid saab ilma suurema ajakuluta kohe rakendada ja kasutama hakata.

Tarkvaratööriista valikul tuleks tähelepanu pöörata sellele, et selle suurus ja liik sobiks institutsioonile. Muudeks olulisteks valikukriteeriumideks võiksid olla tarkvaratööriista rakendatavus, hind ning kasutajatoele ja võimalikele koolitustele tehtavad kulutused. Lisaks neile võiksid valikukriteeriumide hulka kuuluda ka:

- veebitehnoloogiate abil toetatavad platvormid või platvormidest sõltumatus,
- liideste võimalused institutsiooni teiste programmidega, näiteks tõrgete halduseks (help desk) ja hoiatuste andmiseks või inventariseerimis- ja personalitöö programmid,
- kasutajasõbralikkus, eriti dokumendihaldusprogrammide puhul,
- võimalus koostada individuaalseid plaane vastavalt vajadusele, situatsioonile või kasutaja rollile,

- salvestatud ja hallatavate andmete turvalisus ja kaitse (nt isiklikud telefoninumbrid, aadressid),

- käideldavus kriisisituatsioonis (nt juurdepääs interneti kaudu) või

- töökindlus, mis on kriisisituatsioonis eriti oluline, kuna stressiolukorras tuleb arvestada võimalike vigade suurema esinemissagedusega.

Infoturbe seisukohalt esitatakse hädaolukordade haldusprogrammidele järgmisi olulisi nõudeid:

- riist- ja tarkvara peavad olema paigaldatud nii, et oleks võimalik täita käideldavusele ja andmete integreeritusele esitatavaid nõudeid,

- kommunikatsioon oleks võimalik läbi kindlate protokollide, nt administratsiooni poolt ja kaugjuurdepääsuga,

- kasutajahaldus võimaldaks luua kogu institutsiooni hõlmavat hädaolukordade halduse rollikontseptsiooni,

- oleks võimalik usaldusväärne juurdepääsukontroll,

- tootja reageeriks võimalikult kiiresti avastatud turvapuudustele ja pakuks regulaarselt värskendamist ja kiiresti kasutatavaid turvalappe,

- eriti tundlike andmete krüpteerimisvõimalus.

Järgnevalt tuuakse välja mõned eespool nimetatud turvakaalutlustest lähtuvate valikukriteeriumide aspektid.

- Kas tarkvaratööriist toetab kindlaid kommunikatsiooniprotokolle? Selleks, et oleks tagatud turvaline andmevahetus, peavad võrgus töötavad tarkvaratööriistad edastama kindlaid protokolle, brauseril põhineva konfiguratsiooni korral näiteks SSL/TLS-i..

- Kas tarkvaratööriist suudab kasutajat identifitseerida ja autentida?

- Kas tarkvaratööriist võimaldab parooli või teiste autentimistähiste krüpteeritud salvestamist? Pole mõtet soetada tarkvaratööriistu, mis ei võimalda paroole krüpteeritult salvestada.

- Kas toodet ostes pakutakse juurde võimalus sõlmida selle hooldusleping?

- Kas hooldusleping sätestatakse probleemi tekkimisel maksimaalne aeg, mille jooksul tuleb sellele reageerida? Hooldusleping õigustab end ainult siis, kui lisaks garanteeritud reageerimis- ja taastamisajale on lepingus sätestatud ka seadmete käideldavusele esitatavad nõuded.

- Kas tootja pakub kliendile tehnilist nõustamist (hotline), et probleemide ilmnedes kohe abi saada? Vastav punkt tuleks lisada sõlmitavasse hooldusleping. Lepingu sõlmimisel tuleks pöörata tähelepanu sellele, mis keeles tootja hotline-klienditeenindus suhtleb.

- Kui usaldusväärne ja töökindel on toode? Tootja võiks oma kogemustele toetudes ostjat sellest informeerida.

- Kas protokollimisel on detailid konfigureeritavad? Kas protokollimiseks kasutatakse kõiki vajalikke andmeid? Kas juurdepääs protokollitud andmetele on kaitstud? Protokollimise võimalused peaksid vastama vähemalt turvaeeskirjades toodud nõuetele.

Kui kõik soetatavale tootele esitatavad nõudmised on kirja pandud, tuleb välja selgitada, millised müügilolevatest toodetest antud nõuetele vastavad. Mitte iga toode ei vasta korraga kõigile nõudmistele või ei vasta kõigile nõudmistele ühtmoodi hästi. Seepärast tuleks tootele esitatavatest nõudmistest moodustada pingerida. See aitab ühe või teise toote ostmiseks otsust langetada.

12. Sõnastik

Lühendid / Mõisted	Definitsioonid
Häire	Häire andmise eesmärgiks on võimalikult kiiresti pärast kahjutoovate sündmuste algust pädevaid otsustajaid ja töötajaid informeerida, et asuda hädaolukorrad või kriisi likvideerima.
BCM	Business Continuity Management, hädaolukorra tekkides kriitiliste tööprotsesside edasist ühtset juhtimist võimaldav haldusprotsess.
BIA	Business Impact Analyse, hinnanguline analüüs otseste ja kaudsete kahjude kohta, mida võib hädaolukorda või kriis, aga ka ühe või mitme tööprotsessi katkemine institutsioonile tekitada.
CERT	Computer Emergency Response Team, infoturbe spetsialistidest koosnev meeskond, mis tegutseb konkreetsete turvajuhtumine lahendamisel koordineeriva instantsina, väljastab hoiatusi turvaaukude kohta ja pakub neile lahendusi (nn advisories ehk nõuandjad).
Erialane ülesanne	Erialane ülesanne on ametkondade poolt kasutatav mõiste, millega tähistatakse üht tööprotsessi.
Institutsioon	Mõistet „institutsioon" kasutatakse üldmõistena asutuse, ettevõtte või muu organisatsiooni kohta.
Kuum koht (hot site)	„Kuumi kohti" hoitakse aktiivselt pidevalt tegevusvalmina. Ühe asukoha väljalangemisel võib „hot site'i" ilma ajalise viivituseta otsekohe aktiviseerida.
Külm koht (cold site)	„Külmadeks kohtadeks" nimetatakse kohti, kus on olemas küll kõik eeldused IT-süsteemide rakendamiseks, kuid need ei ole veel paigaldatud nii, et need oleksid töövalmid.
KPI	Key Performance Indicator, koodid, mille abil on võimalik määratleda, kas on liigutud püstitatud eesmärgi suunas või kas eesmärk on saavutatud.
Kriisihaldus	Kontseptsiooniliste, organisatsiooniliste ja tehniliste eelduste loomine selleks, et kahjutekitava sündmuse ilmnedes oleks see võimalik kiiresti likvideerida ja tavaolukord taastada. Kriisihalduse eesmärgiks on tagada institutsiooni otsustusvõime ning eesmärgistatud ja koordineeritud tegevus kriisi likvideerimiseks. Kogu institutsiooni hõlmav kriisihaldus on pädev tegelema igat liiki kriisidega. Käesoleva kriisihaldamise standardi mõttes on kriisideks erinevat liiki kriisid. Kriisi likvideerimiseks ei piisa seega ainult ühest komplekssest kriisihaldusest.
Tööprotsesside kriitilisus	Tööprotsesside eskaleeriv hindamine (klassifitseerimine), mille läbiviimisel lähtutakse protsessi olulisusest institutsiooni väärtusloomele. Klassifitseerimisel lähtutakse enamasti tööprotsessi taaskäivitamisele esitatavatest nõuetest või katkestuse kestusega kaasneda võivatest kahjudest, kuid ka teistest kriteeriumitest.
Kriitilised ressursid	Institutsiooni ressursid, mille väljalangemisega kaasneb (kriitiliste) tööprotsesside katkestus või väljalangemine.
Hädaolukorrakeskus	Ruumid, mida kriisistaap kasutab tööruumina ja mille asukoha ja sisseseade kohta kehtivad erinõuded.
MTA	Maksimaalselt vastuvõetav hädaolukorrarežiim
MTPD	Maximum Tolerable Period of Disruption, maksimaalselt vastuvõetav katkestusaeg, mille ületamisel on protsessi või institutsiooni eksistents tõsises ohus.

Hädaolukorrakäsiraamat	Hädaolukorrakäsiraamat sisaldab kogu informatsiooni, mida on vaja hädaolukorra või kriisi ajal ja selle likvideerimiseks. Sellesse on koondatud kõik hädaolukorraga seotud tegevusplaanid nagu näiteks kriisiaja kommunikatsiooni plaan, kriisistaabi tegevusjuhis, taaskäivitamis- ja taastamisplaanid.
Hädaolukorrakontseptsioon	Hädaolukorrakontseptsioon hõlmab hädaolukorraennetuse kontseptsiooni ja hädaolukorrakäsiraamatut.
Hädaolukorraennetuse kontseptsioon	Hädaolukorraennetuse kontseptsioon sisaldab kogu hädaolukordade haldusega seotud informatsiooni, mida ei saa otseselt hädaolukorra likvideerimisel kasutada.
Organisatsiooni allüksus	Institutsiooni loogikast lähtuv üksus. Selle all võib mõista näiteks kohta, osakonda, valdkonda või muud institutsiooni struktuuri osa.
RTO	Recovery Time Objective, protsessi või vajaliku ressursi taaskäivitamisele kuluv aeg. Taaskäivitamisele kuluv maksimaalne aeg peab olema väiksem kui maksimaalne vastuvõetav katkestusaeg.
SLA	Service Level Agreement ehk teenuse taseme leping.
Soe koht (warm site)	„Soojas kohas” on ettevalmistatud riistvara koos kõigi vajalike ühendustega, nii et neid on võimalik pärast konfigureerimist kohe kasutusele võtta, või mis on mõnel muul viisil kasutuselevõtuks ette valmistatud.
Taaskäivitamise aeg	Ajavahemik protsessi katkemise ja hädaolukorrarežiimi käivitumise vahel.
Väärtuste ahel	Väärtuste ahela all mõistetakse seda osa väärtusloome ahelast, mis asub organisatsiooni sees. Väärtusloome ahelasse kuulub toote või teenuse kogu teekond alates tootjast kuni tarbijani ja seepärast võib see hõlmata mitmeid institutsioone.
Taastamisaeg	Taastamisaeg on ajavahemik protsessi katkemisest kuni tavarežiimi alguseni. Taastamisaeg peab olema väiksem või võrdne kindlaksmääratud taaskäivitamisajaga pluss maksimaalne vastuvõetav hädaolukorrarežiimi aeg (taastamisaeg < taaskäivitamise aeg + maksimaalselt vastuvõetav hädaolukorrarežiim).

Teised käesolevas dokumendis kasutatavad mõisted ja lühendid leiate IT-etalonturbe kataloogi sõnastikust.

Lisa A Strateegiavõimalused

Allpool käsitletakse üldjoontes üksikute ressursside olulisi võimalusi. Hinnangu andmiseks ja valiku tegemiseks tuleks igal konkreetsel juhul üksikasjalikult vaadelda ka vastava ettevõte või asutuse võimalusi. Arvestada tuleks ka kohalike teenusepakkujate poolt pakutavaga ning asutuse või ettevõttega seotud riskidega.

Enamiku ressursside puhul saab järgida järgmisi üldisi strateegiad:

sisemiste võimsuste kasutamine,
kooperatiivsed partnerlussuhted ja
sisseostetavate võimsuste ja lahenduste kasutamine.

A.1 Töökohad

Töökohtade järjepidevuse seisukohalt tuleks erinõuetega töökohtade sisseseadmisel arvestada nii tööprotsesside käigushoidmiseks vajalike kontoritöötajate kui ka tootva tööga seotud töötajatega ja tootmisest tulenevate erinõuetega. Valiku tegemisel on otsustavaks taaskäivitamisele kuluv aeg ja võimalike kahjude suurus.

Tegevuse jaotamine
Kui protsessid tuleb taaskäivitada väga lühikese ajaga, tuleks kaaluda, kas jaotada need liiaselt mitme asukoha vahel. Taolistel liiasusega kohtadel toimub tööprotsess samal või sarnasel viisil. Vajalikud ressursid, kaasa arvatud personal, on seal pidevalt olemas. Kasutatavad ressursid on alati samad. Hädaolukorra tekkides võtab hädaolukorrast puutumata koht endale üle väljalangenud koha ülesanded. Seepärast ei ole vaja alternatiivsesse töökohta personali lähetada. Selleks, et tööülesannete ülevõtmine toimuks tõrgeteta, peab tegevuse jaotamine olema ette valmistatud. Muuhulgas tähendab see hädaolukorra korral liiaste andmete hoidmist või andmete ülekandmist. Taoline lahendus on ideaalne juhul, kui taaskäivitamise aeg on väga lühike, sest nii saab ära kasutada aega, mis on vajalik alternatiivsete töökohtade loomiseks, kuid ei sobi eriti juhul, kui otsitakse pikaajalisi võimalusi.

Pidevalt mittetäidetud organisatsioonisisesed töökohad

Kulukaks alternatiiviks on mõnede töökohtade hoidmine erijuhtumiteks. See tähendab, et neid kohti saab vajadusel kohe kasutusele võtta. Vastavalt sellele, kas tegemist on „kuuma" või „sooja" kohaga, on selle alalise valmisoleku kindlustamine seotud märkimisväärsete investeerimiskulude ja jooksvate kulutustega.

Muu ettevõttesisene lahendus

Kui on olemas ruumid, mida tuumtegevuse jaoks ei kasutata või kasutatakse neid vaid aeg-ajalt, võib need hädaolukorra korral lühiajaliselt kasutusele võtta. Taolisteks ruumideks võivad olla näiteks koolitus- ja koosolekuruumid või ka kohvik.

Ressursside vabastamine

Hädaolukorra korral kasutatakse kriitiliste protsesside tööshoidmiseks nende protsesside ressursse, mis on hädaolukorrast puutumata, ja mis on madalama kriitilisuse astmega. Madalama prioriteetsusega protsesse vähendatakse või seisatakse hoopis. Seejuures vabanenud ressursse võib lühiajaliselt kasutada kriitilise protsesside tööshoidmiseks.

Kaugtöökohad ja kaugjuurdepääs

Kui protsessi tööshoidmine ei ole seotud kindla kohaga, võivad töötajad, omades vastavat varustatust ja juurdepääsu internetile, töötada ükskõik kus, ka näiteks kodus. Tuleb jälgida, et institutsiooni võrk või wifi ei oleks üle koormatud. Vajadusel tuleb seda kontrollida. Seejuures tuleb järgida ka muid tingimusi. Kui töötajad töötasid kodus juba ka varem, tuleb kehtestada reeglid töökorralduslikele aspektidele, nagu näiteks turvalisus, tarkvara värskendamine või vajalike dokumentide kasutamine ja nende vahetamine. Tööks vajalik varustatus peaks kaugtöökohal igal juhul dubleeritud olema. Käsiraamatutest, mida kasutatakse korraga nii püsitöökohal institutsioonis kui ka kaugtöökohal, on vähe kasu, sest võimaliku hädaolukorra korral institutsioonis ei ole neid võimalik sealt kätte saada.

Koostöö partnerluse raames

Partnerlussuhted naaberinstitutsioonidega võivad aidata kriisist üle saada. Seda juhul, kui võimaldatakse juurdepääs naabruses asuva institutsiooni ressurssidele ja neid lubatakse lühiajaliselt kasutada. Koostööd tegevatel institutsioonidel peavad olema sarnased struktuurid.

Põhimõtteline valmisolek teha hädaolukorras koostööd tuleb juhtkonna tasandil kokku leppida. Juba varem tuleb jõuda selgusele selles, millises ulatuses on hädaolukorra korral võimalik partneri ruume kasutada, kus need ruumid asuvad ja millised on sealsed arvutid ja milline on võimsus. Hädaolukorra koostöövõimalusi tuleb juba varem kavandada ja sätestada ning iga võimalus organisatsiooni vastavate allüksuste vahel ära proovida, et hädaolukorra korral oldaks nende teostatavuses kindel. Koostööks vajalikud üksikasjad võiks välja töötada hädaolukorrahaldur. Siiski oleks soovitav moodustada kõigi koostööd tegevate institutsioonide hädaolukordade halduse eest vastutajate ühine töörühm. See on ka heaks võimaluseks jagada kogemusi selle kohta, millised on ähvardavad ohud ja strateegiad nende vältimiseks. Pidevalt tuleb jälgida ja vajadusel ümber hinnata riskifaktoreid, turusituatsiooni ja teisi raamtingimusi ja lisada need kokkuleppesse. Vastav kohustus tuleb lepinguga sätestada ja selle täitmist tuleb regulaarselt kontrollida.

Vastastikust kokkulepet on naaberettevõtete vahel valitseva konkurentsi (nt pakkujate sarnased, kuid erineva hinnaga kaubad) tõttu tihti küllalt raske sõlmida. Igal juhul tuleb rakendada kaitsemeetmeid spionaaži ja muude sarnaste ohtude vastu.

Teenusepakkujate kommertslikud lahendused

Tihti valitakse variant, mil kasutatakse nende väliste teenusepakkujate teenuseid, kes on spetsialiseerunud alternatiivsete töökohtade või -teenuste pakkumisele. Hädaolukorra korral pakuvad nad varem sõlmitud lepingus lubatud ressursse selleks, et tööprotsessid täielikult või osaliselt alternatiivsesse töökohta üle viia. Lepingus peavad kokkulepitud teenused üksikasjalikult sätestatud olema. Samuti tuleb lepingus kindlaks määrata trahvid, mida tuleb maksta juhul, kui lepingulisi kohustusi ei täideta kokkulepitud viisil. Kuna taolisi ressursse tuleb vastavalt kokkuleppele hoida pidevalt töökorras, tähendab selline lahendus ka pidevaid kulutusi. Otsus sellise lahenduse kasutamise kohta sõltub kulutuste suurusest ja teenuse kättesaadavuse kriteeriumidest. Siia kuulub nii geograafiline asukoht, koostöö võimalikkus institutsioonidega, kes kasutavad hädaolukorra korral sedasama alternatiivset töökohta, ja vajaliku büroopinna suurus.

Kommertslikke lahendusi võib jagada järgnevalt.

- Kindel alternatiivne töökoht
Organisatsioonivälise teenusepakkuja poolt pakutav kindel alternatiivne töökoht võiks olla sobitatud institutsiooni vajadustega. Olenevalt lepingu tingimustest on sellise töökoha eeliseks asjaolu, et selle kättesaadavus on garanteeritud. Kättesaadavus ja muud lepingutingimused peaksid lähtuma tööprotsesside mõju analüüsist (BIA) ja riskianalüüsist. See variant on küll kulukas, kuid garanteerib kindla alternatiivse töökoha, mida võib hädaolukorra korral piiranguteta kasutada.

- Jagatud alternatiivne töökoht
Erinevalt kindlast alternatiivsest töökohast kasutavad jagatud töökohta ka teised institutsioonid. Olenevalt hädaolukorrast ja selle mõjust võib tekkida olukord, kus alternatiivset töökohta tahab kasutada mitu institutsiooni korraga. Sellisel juhul on töökoht küll olemas, kuid seda saab kasutada kas piiratult või üldse mitte. Seepärast tuleb lepingu sõlmimise läbirääkimistel käigus välja selgitada, kas ja millistel tingimustel saavad ka teised

kliendid valitud alternatiivset töökohta kasutada. Oluline on küsida teenusepakkujalt nende institutsioonide andmeid, kellega koos antud alternatiivset töökohta kasutatakse. Välja tuleb selgitada nende institutsioonide kasutusprioriteedid, aga ka nende tegevusvaldkond ja suurus. Kui teenusepakkuja ei saa tagada, et hädaolukorra korral saab organisatsioon vajalikku alternatiivset töökohta kasutada, tuleks loobuda naabritega ühise asendustöökoha kasutamise võimalusest.

- Mobiilne alternatiivne töökoht
Mobiilseteks alternatiivseks töökohaks nimetatakse näiteks hädaolukorra ajal kasutatavat bürookonteinerit või spetsiaalselt bürooruumiks kohandatud suurveokit. Mobiilne alternatiivne töökoht on töökohtade kadumisel hinna poolest üheks soodsamaks kontorivõimaluseks. Sellise asendustöökoha ruumi suurus on tavaliselt siiski piiratud. Varem tuleks kindlasti kokku leppida kohad, kuhu hädaolukorra korral taolist mobiilset alternatiivset töökohta püstitada. Eelnevalt tuleks ka välja selgitada, kas teenusepakkuja garanteerib elektri- ja muud vajalikud ühendused või peab tellija selle eest ise hoolt kandma.

Hädaolukorra korral võib vaja olla, et töötajad töötaksid kaugtöökohas. Seepärast on oluline välja selgitada, kuidas saaks töötajaid sinna kiiresti ja lihtsasti transportida. Kui töötajaid tuleb pikema perioodi vältel kaugel asuvasse alternatiivsesse töökohta sõidutada ja nad ei saa oma tavalises töökohas töötada, vaid peavad tööl käima teises kohas, tuleb varem selleks personali esinduselt nõusolek küsida. Tuleb kehtestada regulatsioon, kuidas kompenseeritakse töötajate lisaaeg ja -kulutused, mis tekivad seoses alternatiivsele töökohale sõitmisega. Võimaluse korral tuleks juba olemasolevat töölepingut vastavalt täiendada.

A.2 Personal

Tööprotsesside edukaks rakendamiseks vajatakse vastava erialase väljaõppega personali. Sobilikke meetmeid kasutades tuleb kindlustada, et võtmepersonal oleks hädaolukorra korral kättesaadav. See tähendab muuhulgas töötajate asendusregulatsiooni koostamist, samuti tuleb kavandada meetmed, et vajalik personal jõuaks hädaolukorra korral asendustöökohta pärale. Üksikasjalikumat informatsiooni leiate IT-infoturbe kataloogi organisatsiooni- ja personalimoodulist.

Soovitatav on koostada võtmepersonali töökohtade kirjeldused koos nõutava kvalifikatsiooniga ning ülevaade nendest töötajatest ja kvalifikatsioonist, kes toetavad hädaolukorra korral hädaolukorrameeskonna tööd või saavad tänu oma oskustele hädaolukorra korral abiks olla. Siia kuuluvad oskused, mis on seotud

- inimvigastustega (nt esmaabiteadmised)
- hoonetega (nt tuletõrje- või hoonetehnikaeksperdid)
IT või kommunikatsioonivõrkude kahjustustega (nt erialased IT- teadmised).

Erinevate oskuste arendamise treeningud
Töötajate paindliku rollijaotuse hädaolukorra korral tagab spetsiaalselt selleks väljatöötatud treeningprogramm, mille raames koolitakse erinevate valdkondade töötajaid. Nii saavad mitmed institutsiooni töötajad teadmisi, kuidas jooksvat protsessi töös hoida. Sellega välditakse olukorda, kus vastavad teadmised on ainult mõnel üksikul töötajal.

Organisatsioonivälise teenusepakkuja erialase personali kasutamine
Vahel on hädaolukorra korral vaja välist erialast personali kiiresti tööle rakendada. Seepärast oleks soovitav teenusepakkujaga juba varem kooskõlastada võtmepersonalile esitatavad nõuded ja võimalusel sätestada lepingus organisatsioonivälise erialase personali kasutamise tingimused. Kui võõrast personali rakendatakse vaid aeg-ajalt, tuleb läbi viia vastav riskivaatlus ja rakendada sobilikke turvameetmeid.

Teadmiste juhtimine
Selleks, et oma või võõrast personali saaks neile senitundmatute protsesside juures rakendada, on vaja hästi funktsioneerivat ja aktiivset teadmiste juhtimist. Selleks on soovitav kasutada spetsiaalselt praktikale orienteeritud käsitsusjuhendeid ja probleemlahendeid. Kogutud informatsioon tuleks lähtuvalt selle kaitsmise vajadusest astmeti liigitada. On tarvis rakendada vajalikke turvameetmeid. Andmekaitsemeetmete rakendamine peaks tagama juurdepääsu andmetele.

A.3 Infotehnoloogia

Enamik tööprotsesse sõltub informatsiooni- ja kommunikatsioonitehnoloogiast. Eriti oluline koht on seejuures just IT-komponentidel. Järgnevalt antakse ülevaade infotehnoloogia võimalikest jätkustrateegiatest, eriti selles suhtes, mis puudutab arvutuskeskuste käitlemist.

Piiratud IT-käitlemine
Tööprotsesside mõjuanalüüsi (BIA) koostamisel määratletakse ja esitatakse kirjalikult miinimumnõuded ressurssidele, mida hädaolukorra korral vajatakse, aga ka prioriteedid vajalike ressursside taaskäivitamiseks. Tööprotsesse hoitakse käigus väiksema võimsusega ja seega ka väiksemate ressurssidega.

Liiasusega IT-asukohad
Kesksete IT-komponentide paigaldamiseks vajatakse nt serveritele ja arvutuskeskustele eraldi ruume. Liiasusega IT-asukohtadel võivad vastavalt taaskäivitamise ajale olla erinevad modifikatsioonid:

Külm koht (Cold Site)
Mõistega „külm koht" tähistatakse asendustöökohti, kus on küll ruumid, kuid kus ei ole vajalikke IT-komponente. Neis ruumides on olemas vajalikud eeldused IT-komponentide paigaldamiseks, näiteks kliimaseade, või mõnede IT-komponentide eripäraga sobiv vooluvõrk. Hädaolukorra korral viiakse tark- ja riistvara ning andmed alternatiivsesse töökohta üle ja paigaldatakse. Samuti luuakse vajalikud kommunikatsiooniühendused.

Soe koht (Warm Site)
„Soojaks kohaks" nimetatakse alternatiivset töökohta, kuhu on juba varem paigaldatud tarkvara koos kõigi vajalike ühendustega. Tarkvara on paigaldatud nii, et hädaolukorra korral tuleb see ainult aktiveerida ja konfigureerida. Andmebaas tuleb aga alles sisestada. Olenevalt koha komplekssusest ja andmete hulgast võib „soojas kohas" tööd alustada juba mõne tunni pärast.

Kuum koht (Hot Site)
„Kuum koht" on alternatiivne töökoht, kus on täielikult töövõimeline infrastruktuur koos asjakohaste andmebaasiga. Põhitöökoha äralangemisel võib „kuuma koha" kohe aktiveerida (ka kaugjuhtimise teel) ning nii võib seal minimaalse ajakaoga tööülesannete täitmist jätkata. Tavaliselt on siiski vaja, et pädev personal tuleks põhitöökohast sinna üle.

Nõuandeid, milline oleks liiasusega arvutuskeskuste sobilik vahemaa põhikohast, leiab BSI publikatsioonist „Nõuandeid liiasusega arvutuskeskuste asukohtade ruumiliseks vahekauguseks".

Jagatud IT-asukohad
Alternatiiviks liiasusega IT-asukohale on protsesside jaotamine kahe või isegi mitme asukoha vahel. Alternatiivset asukohta ei aktiveerita alles hädaolukorra korral, vaid mõlemaid kohti hoitakse paralleelselt ja tulemuslikult töös. Nii vähendatakse riske, aga ka aega kulub vähem, sest alternatiivset töökohta ei pea eraldi aktiveerima.

A.4 Komponentide hädaolukorrad

Üksikute komponentide hädaolukorra korral on lisaks nende parandamisele käideldavuse tõstmiseks ja võimalikult kiiresti töövõime taastamiseks ka muid võimalusi. Komponentideks võivad olla näiteks server, töökoha arvuti, printer, koopiamasin või telefon, aga ka kliimaseade, hädaolukorrageneraator või tootmisseadmete osad.

Komponentide ladustamine
Eriti kriitilistele komponentidele võib juba varem soetada vajalikul hulgal asendusosi või varukomponente. Siinjuures tuleks aga silmas pidada, et sel juhul on vaja eraldi ladustamisruumi, kuhu sobiks ladustada IT- või teisi tarkvarakomponente, nagu näiteks tootmisseadmete osi. Võimalusel ei tohiks asendussüsteemide ladu asuda samas hooneosas. Minimaalse nõudena peaks see paiknema teises tuletõkketsoonis. Ladustatud komponendid

peavad vastama kasutusel olevatele või olema nendega ühildatavad, seepärast tuleb neid regulaarselt uuendada. Varude hoidmine on kulukas ja võib põhjustada vigu.

Asenduskomponentide soetamine
Kui tööst väljalangenud komponente ei ole võimalik mõistliku ajaga parandada lasta, tuleks nad asendada. Selleks, et soetamisprotsessi kiirendada, peaks olemas olema pidevalt värskendatud asendusosade soetamise plaan, kus oleks iga olulise komponendi kohta piisavalt andmeid (nii töövõime kui tootja ja tarnija kohta). Kui ühte komponenti toodab või tarnib mitu ettevõtet, tuleks nad kõik kirja panna, et hädaolukorra korral saaks valida kiireima tarnija.

Kokkulepped tarnijaga
Paljud tarkvaramüüjad pakuvad lepinguid, milles sätestatakse, et nad garanteerivad asendustarkvara tarnimise võimalikult kiiresti ja seda ka väljaspool üldist tavatööaega. Lepingutes tuleks aga sätestada ka aeg, mille jooksul peab protsessid taaskäivitama. Juhul, kui jõutakse taolise lepingu sõlmimiseni, tuleks tähelepanu pöörata geograafilisest asukohast tuleneda võivale riskile. Lähestikku asuvad institutsioonid võivad katastroofide korral tegutseda ühesuguse kriisistsenaariumi järgi ja on võimalik, et nad vajavad ka samasugust tarkvara, nii et vaatamata sõlmitud lepingutele võib tekkida olukord, kus tarne viibib. Kõrge nõudlusega asendusosa puhul tuleb seepärast lepingusse sätestada ka see, millega toimub tarne transport, näiteks laeva või lennukiga. Siiski tuleks kõigepealt selgusele jõuda, kas tarnija on üldse suuteline igast geograafilisest asukohast asendustarkvara tarnima.

A.5 Info

Ettevõtete ja asutuste infot leidub nii paberkandjatel, elektrooniliselt salvestatuna arvutis kui ka töötajate peades, kokkulepitud toimimismustrites ja tootmisseadmete ehitusviisis. Käesolevas dokumendis mõistetakse informatsiooni all digitaalselt salvestatud teavet ja paberdokumente.

Infoturbe põhiväärtused
Informatsioonil on eriline väärtus, seepärast tuleb teabe jätkusuutlikkuse kõrval tähelepanu pöörata ka infoturbe klassikalistele põhiväärtustele.

- Konfidentsiaalsus
Hädaolukorra korral võib olla ohus mitte ainult teabe kättesaadavus, vaid ka selle konfidentsiaalsus. Nii näiteks peetakse tulekahju korral tihti esmatähtsaks inimeste ja hoonete, mitte aga informatsiooni päästmist. Seepärast võib juhtuda, et konfidentsiaalne info ladustatakse päästetööde käigus tänavale või mõnda teise ajutisse kohta, kus kõrvalised isikud saavad sellele juurdepääsu. Samuti tuleb kindlustada, et hädaolukorra ajal lühiajaliselt rakendatud võõral tööjõul ei oleks konfidentsiaalsele informatsioonile õigustamatut juurdepääsuvõimalust.

- Integreeritus
Hädaolukorra korral võib olla ohus ka informatsiooni integreeritus. Kui teha varukoopiad alles pärast hädaolukorra puhkemist, võivad need osutuda vigaseks. Eriti puudutab see andmepanku, kui tehingulogisid ei ole kindlustatud või kui neid ei ole täielikult kindlustatud, kuna see põhjustab vigu andmepankades. Kuid lünki võib dokumentatsiooni tekkida ka paberdokumentide hävimisel (nt tulekahju või veekahjustuste tõttu).

- Kättesaadavus
Hädaolukorra korral peab institutsiooni tööprotsesside ja nende taastamise teave olema kiiresti kättesaadav. Seepärast tuleb hädaolukordasid puudutavat teavet sobilike meetmete rakendamisega kättesaadavana hoida. Näiteks võib seda hoida dubleerituna erinevates kohtades.

Andmevarundus, andmete hoiustamine ja arhiveerimine
Olenevalt andmepankade kriitilisusest ja nende kättesaadavusele esitatavatest nõuetest esitatakse varukoopiatele erinevaid nõudmisi.

Kui varukoopiaid on vaja kasutada väga kiiresti, võiks kasutada erinevaid liiasuse meetmeid (vt ka IT-infoturbe kataloogi B moodul 1.4 Andmevarunduskontseptsioon) nagu näiteks mirror- või peegelmeetod (shadowing). Selle abil on võimalik andmeid sünkroonselt või ka asünkroonselt liiasesse kohta üle viia või salvestada. Muud liiase andmesäilitamise võimalused, mis võiksid kaasa aidata sellele, et seadusega või lepinguga ettenähtud tiraažist ja arhiveerimisele esitatavatest nõudmistest kinni peetaks, on järgmised.

- Analooginformatsioon
Analooginformatsiooni, nagu näiteks paberdokumente või mikrofilme, võib kopeerida. Neid võib säilitada turvalistes laoruumides. Sobilik meetod paberkandjal oleva teabe liiaseks säilitamiseks on see digitaliseerida või salvestada elektroonilisse arhiveerimissüsteemi.

- Digitaalinformatsioon
Digitaalinformatsiooni võib kopeerida odavamatele andmekandjatele ja seda turvalises kohas säilitada. Seejuures tuleb tähelepanu pöörata sellele, et säilituskoht oleks valitud nii, et see oleks põhikohast piisavalt kaugel ja teisalt piisavalt lähedal, et andmeteni oleks võimalik jõuda ja et nad oleks võimalik kindlaksmääratud taaskäivitamisajaks taastada. Varukoopiate arhiveerimisruumid peavad vastama samadele nõudmistele mis ruumid, kus töödeldakse originaalandmeid.

A.6 Välised teenusepakkujad ja tarnijad

Mõnes kohas on välised teenusepakkujad ja tarnijad tööprotsessidesse niivõrd kaasatud, et kui teenusepakkuja äkki ära langeb, ei saa protsesse enam nõuetekohaselt käidelda. Selle põhjuseks võib olla hädaolukorra, aga ka teenusepakkuja maksejõuetus või lepingu ootamatu ülesütlemine, näiteks puuduliku teenuse tõttu. Võimalikud jätkustrateegiad on sel juhul järgmised.

- Väliste teenuste ülekandmine sisemisteks
Kui teenuseid, mida osutab väline teenusepakkuja, saab osutada ka organisatsioonisisene personal, võib olla kasu sellest, kui teenuste osutamine kantakse kiiresti üle oma institutsiooni. See aga tähendab, et organisatsioonisisesel personalil peaksid olema vajalikud teadmised ja nad tuleb muudest tööülesannetest vabastada. Samuti peab protsesside jaoks vajalik infrastruktuur olemas olema.

- Liiased või alternatiivsed teenusepakkujad
Institutsiooni tööks väga vajalikke teenuseid, nagu näiteks kommunikatsioone või elektriga varustatust, võiks lisaks esmasele teenusepakkujale osutada ka liiane või alternatiivne teenuspakkuja. Siinjuures on oluline, et sellise teenusepakkuja valikul peetaks silmas, et tema asukoht oleks esmasest teenusepakkujast geograafiliselt sõltumatu ja et ta oleks võimeline täitma kindlaksmääratud taaskäivitamisaja nõuet.

Lisa B Ennetavad meetmed

Ennetuseks võivad institutsioonid rakendada erinevat liiki meetmeid. Mõningatest neist on juttu allpool.

B.1 Teavitamise tehnoloogia

Erinevate ohtude varajaseks avastamiseks on olemas erinevad automaatsed ohuteavitusseadmed. Siia kuuluvad näiteks suitsu-, tulekahju-, vee- või liikumisandur.

Automaatsete teavitusseadmete ülesandeks on tuvastada erinevaid parameetreid, mis viitavad otsesele või kaudsele võimalikku kahju toovale sündmusele nii varakult kui võimalik. Samuti peavad nad edastama vastava teade, et vastumeetmed oleks võimalik õigeaegselt tarvitusele võtta. Teade tuvastatud sündmuse kohta edastatakse sel juhul vastavasse keskusesse, näiteks institutsiooni juhtkonnale või teenusepakkujale. Olenevalt ohu liigist, näiteks tulekahju korral, võib olla otstarbekas hoiatada ka kogu ümbruskonda.

Teavitusseadmete hankimisel tuleks järgida eesmärki, et seade aitaks tõsta sündmuse avastamise tõenäosust, teavitaks ohtlikust sündmusest kiiresti, aga aitaks ka erinevate valdkondade pädevatel isikutel otsustada, kuidas reageerida. Teavitustehnika peaks hõlmama kolme valdkonda.

- Territooriumi valve
Territooriumi valvamiseks on kolm olulisemat sensori liiki: liikumissensor (nt infrapunakiirel põhinev valve, hermeetiline videovalve), piirdesensor ja maapinna sensor (nt maapinna tõuke andur).

- Siseruumide valve
Siseruumide valve hõlmab ala alates hoone välisküljest kuni kaitsealuse objektini. Esmalt tuleks dokumenteerida, millised nõudmisi igale valvatavale alale esitatakse ja vastavalt sellele tuleb paigutada sensorid.

- Objekti valve
Mõnda objekti on vaja eraldi valvata. Siia kuuluvad näiteks temperatuurikõikumine serverikappides või IT-komponentide töö.

Olenevalt valveülesannetest võib teavitussüsteeme liigitada nende paigutuskoha, funktsiooni ja neile esitatavate nõudmiste järgi. Enne teavitussüsteemi paigaldamist tuleks pöörata tähelepanu järgmistele punktidele:

- ümbruse parameetrid,
- energiavarustus,
- segavad mõjud,
- nendest ülesaamise võimalus,
- kasutajasõbralik käsitsus ja hooldamine.

Ohuteavitusseade koosneb paljudest väikestest anduritest. Need on ühendatud keskusega, kuhu saadetakse signaal ja kus käivitub alarm. Kui liikumis-, tulekahju-, vee- või gaasiandur on juba olemas, tuleb need vähemalt institutsiooni tuumikalal siduda valvesüsteemiga. Nii saab ohte varakult tuvastada ja vastumeetmed tarvitusele võtta. Teated või signaalid peavad jõudma kohta, kus on olemas alaline inimvalve (väravavaht, valve- ja turvateenistus, tuletõrje jne). Seejuures tuleb tagada, et koht, kuhu signaal või teade saadetakse, oleks võimeline hoiatusele reageerima (nii tehniliselt kui ka inimressursi poolest).

Ohuteavitusseade on kompleksne terviksüsteem, mida on võimalik sobitada nii kogu hoone kui üksikute tööprotsessidega, kuid selle soetamisel ja paigaldamisel tuleb siiski silmas pidada, et ta vastaks institutsiooni vajadustele.

Hoiatus peaks kanduma keskse pädeva üksuseni. Oleks otstarbekas, kui ohuteavitusseade oleks integreeritud institutsiooni juhtimis- ja kommunikatsioonisüsteemi. Olenevalt paigaldatud valvesensoritest ja välistest parameetritest peaksid institutsiooni pädeva üksuse töötajatel olema järgmised tehnilised seadmed:

- kõigi videovalvemonitoride asendiplaan,

- suure ekraaniga arvutid protokollimiseks, et oleks garanteeritud, et stressisituatsioonis ei tehta informatsiooni edastamisel vigu,

- telefoni- ja faksiühendus,

- võimalusel telefon, millel oleks otseühendus valvetöötajatega (tuletõrje, politsei),

- raadiosidekeskus, millel on otseühendus valvetöötajate mobiiltelefonidega (reservraadiosideaparaadid, mida valvetöötajad hädaolukorra korral kasutada võivad),

- plaanide, jooniste ja objektispetsiifiliste dokumentide (asendiplaanid) arhiiv.

Selleks, et tulevikus oleks võimalik meetmeid kavandada ja nende mõjusust hinnata, on oluline kõik ohuteavitusseadmete saadetud turvajuhtumeid puudutavad teated üksikajalikult dokumenteerida ja neid analüüsida. Taolist informatsiooni saavad anda nii inimesed (mis nad on nt valvekäikude ajal kogunud) kui ka infosüsteemid. Dokumenteerida tuleks järgmist informatsiooni:

- inimeste või andurite poolt saadetud teated,
- aruanded kahju tekitanud sündmuste ja kahjude kõrvaldamise kohta,
- hoiatusteated,
- vajalikud reageerimismeetmed,
- objekti ja tegevust puudutav lisainformatsioon (nt plaanid ja kontrollnimekirjad).

Lisaks tuleb dokumenteerida andmed, mis on varem viidanud juba toimunud ja kahju toonud sündmusele, et sarnase olukorra taastekkimise puhul oleksid vajalikud teadmised olemas.

B.2 Andmevarundus

Iga institutsiooni jaoks on informatsioon tähtis, olenemata sellest, kas ta on olemas analoogsel või digitaalsel kujul. Kui materiaalsed ressursid hävivad või muutuvad kasutamiskõlbamatuks, saab neid enamasti tarnijate või väliste teenusepakkujate abiga või mõnel muul viisil taastada. Andmekandjatele salvestatud informatsioon on aga omand, mis läheb andmekandja hävimisel või kahjustamisel kaduma. Seepärast tuleb andmete kaitseks rakendada erimeetmeid.

Nagu IT-infoturbe kataloogi moodulis B 1.4 Andmevarunduskontseptsioon kirjeldatud, on oluline, et institutsiooni sees koostataks andmevarunduse kontseptsioon.

B.3 Lepped väliste teenusepakkujatega

Kui jätkustrateegias on ette nähtud, et hädaolukorra likvideerimiseks kasutatakse ka kommertslike teenuspakkujate hädaolukorra likvideerimisteenused siis, tuleb teenusepakkujate valikul ja lepingute koostamisel lähtuda samadest kriteeriumidest nagu väljasttellimise puhul. Selle olulisemaid punkte kirjeldatakse IT-infoturbe kataloogi moodulis B 1.11 Väljasttellimine.

Hädaolukorraks valmisolekuks pakutakse mitmeid teenuseid, nagu näiteks hädaolukorra arvutuskeskuseid, erinevaid aplikatsioone või IT-komponente, kuid ka alternatiivseid töökohti või erinevate valdkondade pädevat personali. Kui institutsioon on otsustanud kasutada

hädaolukorra puhuks mõeldud teenuseid, tuleb kõigepealt määratleda, millised on taolistele teenustele esitatavad nõudmised. Teenusepakkuja valitakse vastavalt nõudmistele.

Seepärast on enne teenusepakkuja valimist oluline määratleda kriteeriumid, millele ta peaks vastama. Leping sõlmitakse teenusepakkujaga, kes vastab kõigile esitatud nõuetele.

Enne seda tuleks aga küsida erinevate pakkujate hinnapakkumisi. Selleks puhuks oleks soovitatav sisse seada nn kohustuste teatmik, kuhu oleks võimalik kirja panna teenused, mida institutsioon soovib osta. Taolise teatmiku abil on hiljem hea pakkumisi hinnata ja pakkujate vahel valikut teha. Sellest on abi ka tulevikus sõlmitavate lepingute korral. Seetõttu on oluline kõik vajaminevad teenused üksikasjalikult kirja panna. Sellega tagatakse, et kokkulepitavad teenused katavad täielikult kõiki kriitilisi tööprotsesse. Kohustuste teatmikus peaksid olema kajastatud institutsiooni kõik pädevad allüksused ja nende rollid.. Allüksused ja nende rollid võivad näiteks olla järgmised.

- Hoone haldus;
- Hädaolukordade halduse planeerimise eest vastutamine;
- Infotehnoloogia töötaja; soetamine
- Õigusosakond; ostmine

Soovitatav on koostada ka küsimuste katalooge, kuhu märkida teenusepakkujatele esitatavad nõudmised. See võiks sisaldada näiteks järgmisi punkte.

- Pädevusvaldkond, teenusepakkuja suurus ja asukoht
- Teenusepakkuja soovitajad
- Kvaliteeditõend või sertifikaat, nt IT-infoturve ISO 27001 järgi
- Hädaolukordade halduse juhtimiseks ja hädaolukorra likvideerimiseks pakutavad teenused
- Testimise ja harjutamise võimalus
- Ühekordsed kulud, aastased kulud, rakendamiskulud, testidest ja harjutustest osavõtmise kulud
- Teenusepakkuja võime tellija soovidega kohanduda
- Ressurssidest tulenevad nõudmised (garanteeritud tegevusse asumise aeg, reageerimisaeg jne)
- Kommunikatsiooniliidesed
- Teenusepakkuja põhjendatud turva- ja hädaolukorraennetuse kontseptsioon
- Võimalused oma auditi läbiviimiseks

Nõuete profiil sõltub paljugi sellest, millist liiki hädaolukorrateenuseid soovitakse kasutada. Väärtuskriteeriume tuleks sobitada konkreetsete asjaoludega ja neid tuleks üksikult kaaluda.

Kui on langetatud otsus ühe teenusepakkuja kasuks, tuleb lepingus sätestada kõik hädaolukordade halduse kriteeriumid. Samuti peaksid lepingus olema kirjas koostööst tulenevad asjaolud, nt kontaktisikud, töötajate asendamine, reageerimisajad, IT-ühendused, osutatavate teenuste kontrollimine, IT-turvameetmete väljatöötamine, konfidentsiaalsete andmete töötlemine, kasutamisõigused, dokumentatsiooniga seotud kohustused ja info edastamine kolmandatele isikutele.

B.4 Alternatiivsete töökohtade määratlemine ja neile esitatavad nõuded

Hädaolukorra ennetamise kavandamise käigus tuleb mõne stsenaariumi korral välja valida kas üks või mitu alternatiivset töökohta, seda nii büroo, tootmise kui ka IT jaoks.

Hädaolukorraennetamise kontseptsiooni väljatöötamisel tuleks arvestada järgmiste punktidega:

- Alternatiivse töökoha kättesaadavus (liiklusvahendid ja teed) ja vajadusel töötajate transport.

- Alternatiivse töökoha sisseseade (töökohtade arv, infrastruktuur, turvameetmed, nt juurdepääsu kaitse).

- Kommunikatsioonikanalid ja -vahendid (telefoniühenduste vajadus, telefonide ja fakside ümberlülitamine, vähim vajadus telefoni- ja faksiühenduste ja -seadmete järele).

- Alternatiivsete töökohtade võrguühendus (nt WAN-ühendus oma arvutuskeskusesse või IT-ühendus interneti kaudu). Tuleks teada andmete läbilaskevõimet, IP-aadresse, turvameetmeid, tuletõkkesüsteemi liiki ja konfiguratsiooni jne.

- Töötajate ja nende asendajate kättesaadavus alternatiivsel töökohal ja/või kodus (telefoni- ja mobiilinumber, meiliaadress).

- Alternatiivse töökoha kasutuselevõtmise meetmed ja isikud, kes vastutavad selle eest, et antud kohas saaks nõutud ajal tööd alustada.

- Pärast hädaolukorra kõrvaldamist alternatiivse töökoha likvideerimise meetmed ja isikud, kes vastutavad selle eest, st kelle pädevusse kuulub see, et alternatiivsel töökohal taastataks seal enne hädaolukordad valitsenud olukord. Siia kuulub näiteks telefonide ümberlülitamine või ka IP-aadresside ümberseadistamine.

Lisa C Hädaolukorrakäsiraamatu struktuur

Hädaolukorrakäsiraamatu struktuur peaks olema selline, et selle koostamisel mitteosalenud pädev isik oleks võimeline käsiraamatus käsitletud meetmeid rakendama. Näitena tuuakse allpool ära ühe hädaolukorrakäsiraamatu sisukord. See, milliseid toodud struktuurijaotusi üle võtta, sõltub olemasolevast süsteemi- ja kasutusdokumentatsioonist ning seepärast tuleb selle üle eraldi otsustada.

Nõuanne: institutsiooni hädaolukorrakäsiraamatu ülesehitus ja struktuur sõltub institutsiooni suurusest ja struktuurist. Allpool olev struktuur on vaid üheks näiteks ning tuleb sobitada konkreetse institutsiooni tingimustega.

1 Sissejuhatus
- 1.1 Üldine informatsioon: organisatsiooni nimi, kehtivusala, jne
- 1.2 Dokumendid: versioon, saajad, dokumentatsiooni eest vastutajad, dokumentide liigitus jne
- 1.3 Kasutatavad lühendid

2 Kiirmeetmed
- 2.1 Üksikute isikute ülesanded / nende tegevus hädaolukorra korral
- 2.2 Tegevusjuhised erinevateks hädaolukordadeks

3 Kriisihaldus
- 3.1 Rollid, pädevusvaldkond ja kompetents
- 3.2 Teadete edastamine ja eskalatsioon
- 3.3 Kriisistaabi ruum / laokeskus
  - 3.3.1 Asukohad, kättesaadavus ...
  - 3.3.2 Hädaolukorraaegse kohtumispaiga ettevalmistamine
- 3.4 Kriisistaabi töö
- 3.5 Hinnang olukorrale
- 3.6 Kriisistaabi dokumentatsioon
- 3.7 Deeskalatsioon
- 3.8 Hädaolukorra likvideerimise analüüs ja hinnang

4 Kriisiaegne kommunikatsioon ja töö avalikkusega

5 Taastamine
- 5.1 Büroopinna taastamine
- 5.2 Infrastruktuuri taastamine
- 5.3 IT taastamine
- 5.4 Kommunikatsioonide taastamine

6 Tööprotsesside jätkamine
- 6.1 Organisatsiooni allüksuste kättesaadavusele esitatavad nõuded
- 6.2 Plaanid tööprotsesside jätkamiseks
  - 6.2.1 Organisatsiooni A-kriitilisusega allüksused
  - 6.2.2 Organisatsiooni B-kriitilisusega allüksused
  - 6.2.3 Organisatsiooni C-kriitilisusega allüksused
- 6.3 Protsesside taaskäivitamise ja taastamise analüüs

7 Lisad

7.1 Hädaolukorrameeskonna liikmete kättesaadavus

7.2 Hädaabinumbrid (nt tuletõrje, politsei, kiirabi, vee- ja elektriettevõte, alternatiivse töökoha arvutuskeskus, väljapool institutsiooni asuv andmekandjate arhiiv, organisatsiooniväline telekommunikatsiooniteenuse pakkuja)

7.3 Muud olulised plaanid ja nimekirjad

Lisa D Tööprotsesside jätkamise plaani struktuur

Järgnevalt tuuakse näitena ära tööprotsesside jätkamise plaani võimalik struktuur. See, milliseid jaotusi kasutada, oleneb institutsiooni ja tööprotsesside ülesehitusest ja selle üle tuleb eraldi otsustada.

1 Sissejuhatus

- Üldine informatsioon: organisatsiooni nimi, plaani nimetus, plaani eesmärk, kehtivusala jne
  - Plaani aktiveerimine ja desaktiveerimine
  - Dokumendid: versioon, saajad, dokumentatsiooni eest vastutajad, dokumentide liigitus jne
  - Kasutatavad lühendid
  - Põhi- ja lisadokumendid

2 Organisatsiooni allüksuse töö hädaolukorra korral

- Vastutaja
- Hädaolukorrameeskond, selle kohustused ja pädevus
- Hoiatamine ja eskalatsioon

3 Tööprotsesside taaskäivitamine

- Taaskäivitamise strateegia
- Taaskäivitamise eesmärk ja maksimaalne hädaolukorraolukorras töötamise aeg
- Protsesside ressursinõudmised
- Alternatiivid hädaolukorraolukorras ja alternatiivsel režiimil töötamisele
- Endiste tööprotsesside taastamine
- Hädaolukorrajärgne analüüs

4 Stsenaariumid

- Stsenaarium „hädaolukorra töökohas”
  - Alternatiivsele töökohale esitatavad nõuded
  - Alternatiivsel töökohal nõutavad ressursid
  - Reaktiivsed taaskäivitamismeetmed
  - Tööprotsessi muudatused hädaolukorrarežiimil töötamisel
  - Tavarežiimi taastamise ja sellele ülemineku meetmed
- Stsenaarium „Infotehnoloogiline hädaolukord”
  - Jätkustsenaariumid
  - Hädaolukorrarežiimil töötamise nõuded
  - „Vastava rakenduse / vastava süsteemi jälgimine”
  - Asendustarvikute soetamise plaan
- Stsenaarium „Personaliga seotud hädaolukord”
  - Jätkustsenaariumid
  - Hädaolukorrarežiimil töötamise nõuded
  - Reaktiivsed taaskäivitamismeetmed
  - Tööprotsesside muudatused hädaolukorrarežiimil töötamisel

- O Tavarežiimi taastamise ja sellele ülemineku meetmed
- Stsenaarium „Teenusepakkujaga seotud hädaolukord”
  - o Jätkustsenaariumid
  - o Reaktiivsed taaskäivitamismeetmed
  - o Tööprotsesside muudatused hädaolukorrarežiimil töötamisel
  - o Tavarežiimi taastamise ja sellele ülemineku meetmed

5 Lisainformatsioon

- Asukohad
- Juuresõiduplaanid

6 Kontaktinfo

- Töötajate nimekiri
- Teenusepakkujad
-

7 Lisa

- Formularid, näidised, kontrollnimekirjad,

Soovitatavad dokumendid

Tänusõnad

Käesoleva juhendi koostamist toetasid Saksa Infotehnoloogia Turbe Ameti eksperdid, kes jagasid koostajatele oma praktilisi teadmisi. Olgu tänatud kõik need, tänu kellele sai juhendi koostamine võimalikuks.

BSI standard 100-4 põhineb ettevalmistaval tööl, mille tegi BSI tellimisel firma HiSolutions AG. Suur tänu Robert Kallwiesile, Timo Kobile, Stefan Neesile ja Björn Schmelterile abi eest.

Täname ka eksperte ja institutsioone, kes andsid oma kirjutiste ning kasulike nõuannetega väärtuslikke tõukeid käesoleva juhendi valmimiseks. Teile kuulub meie eriline tänu, sest tänu teie abile ja toetusele sai käesoleva standardi valmimine võimalikuks.

- Thomas Bittl, Posti ja Telekommunikatsiooni Föderaalamet
- consequa GmbH
- Ulrich Dreyer, 3R-Kontext
- Ingo Geisler, Vodafone D2 GmbH
- Matthias Hämmerle, KPMG AG
- Dr. Armin Hampel, Hewlett-Packard

GmbH

- Dr. Wolfgang Mahr, Axept AG
- Michael Müller, KPMG AG
- Uwe Naujoks, UKN Management Consulting
- Markus Riedl, Bayer. Saksa Siseministeerium
- Thomas Teichmann, Schmitz & Teichmann Betriebsberatung GmbH
- Astrid Wiesendorf, Vodafone D2 GmbH

BSI standardi 100-4 koostamisel osalesid järgmised BSI töötajad: dr Marie-Luise Moschgath, Isabel Münch, dr Harald Niggemann.