Zaštita i sigurnost informacijskih sustava

Planiranje kontinuiteta poslovanja za nepredviđene slučajeve

prof. dr. sc. Krešimir Fertalj

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.

Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

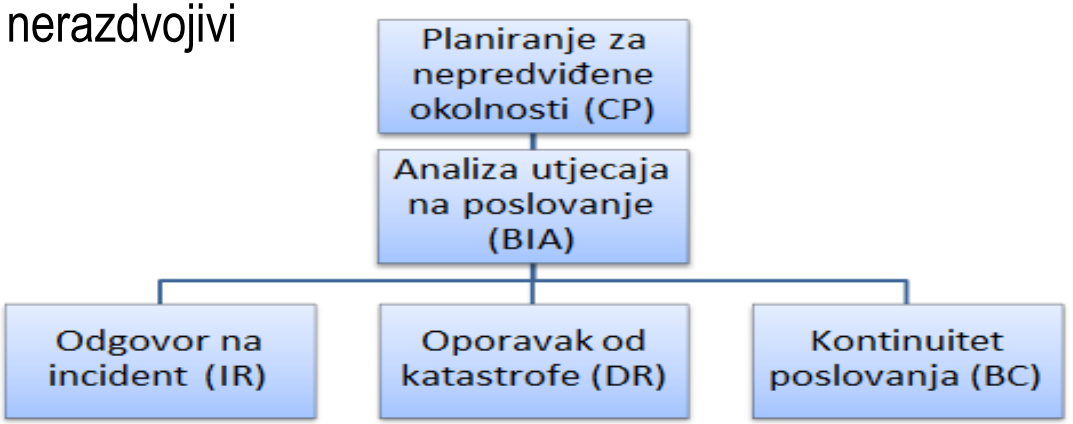
Tekst licencije preuzet je s http://creativecommons.org/.

Osnovni pojmovi

- Štetni događaj (adverse event)
  - Događaj s negativnim posljedicama koji bi mogao ugroziti resurse ili operacije organizacije – napad, sabotaža, potres, poplava, požar, curenje plina, radijacija, …
  - Mogući kandidat za incident
- Incident
  - Štetni događaj koji može rezultirati gubitkom informacijske imovine, ali trenutno ne prijeti održivosti čitave organizacije
  - Jasno identificirani napad na informacijsku imovinu koji može ugroziti njenu povjerljivost, cjelovitost ili raspoloživost
- Katastrofa (disaster)
  - Štetni događaj koji bi mogao ugroziti održivost čitave organizacije
  - Eskalira iz incidenta ili odmah bude proglašena

Planiranje za nepredviđene situacije

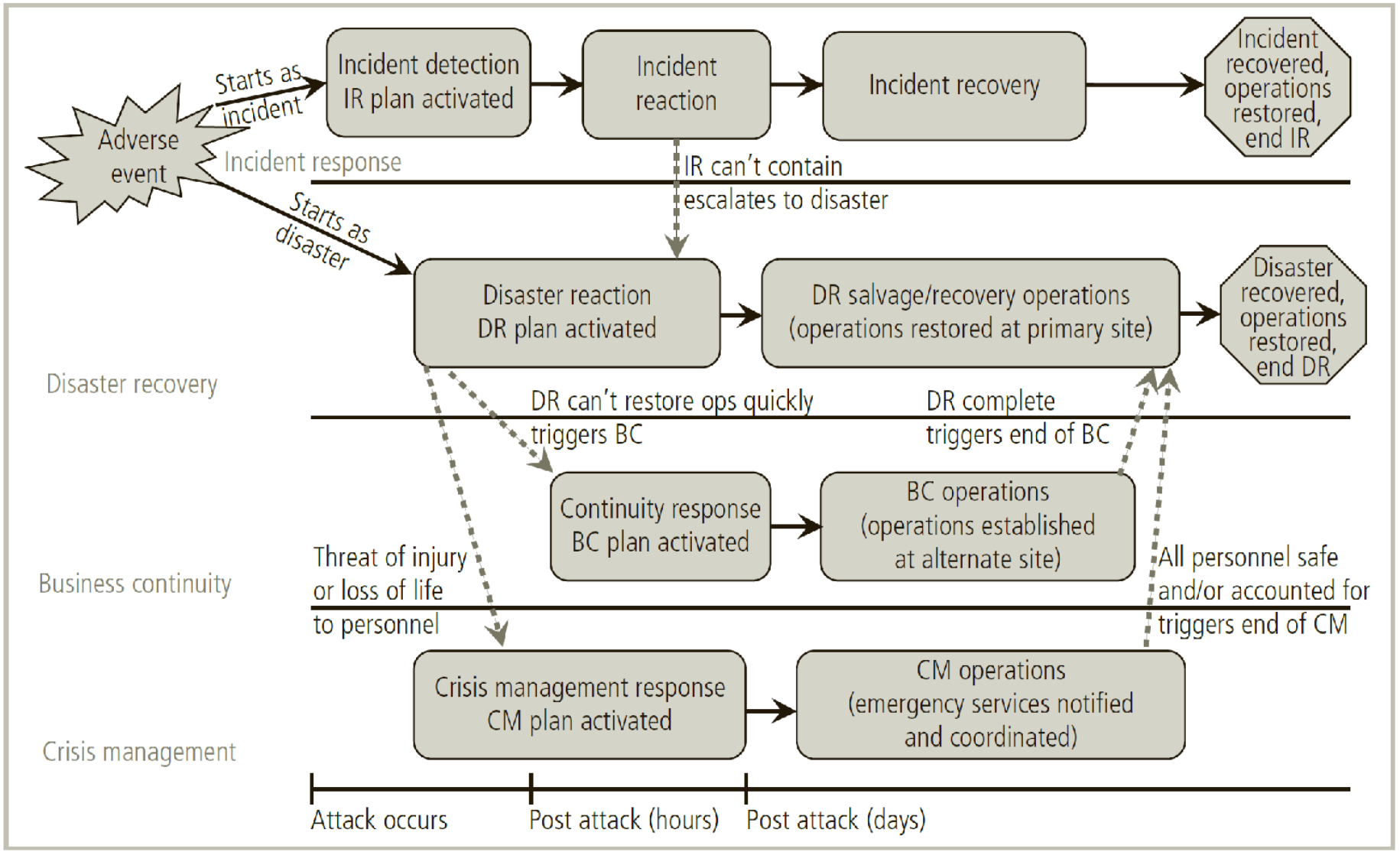
- Planiranje za nepredviđene situacije (Contingency planning - CP)
  - više rukovodstvo odredi što kada štetni događaj postane incident ili katastrofa
- Elementi
  - Analiza utjecaja na poslovanje (Business Impact Analysis - BIA)
  - Planiranje odgovora na incidente (IR), oporavka od katastrofe (DR) i kontinuiteta poslovanja (BC)
    - Planiranje nastavka poslovanja (Business Resumption Planning – BRP) = DRP + BCP
    - Smatra se da su planovi DR i BC nerazdvojivi

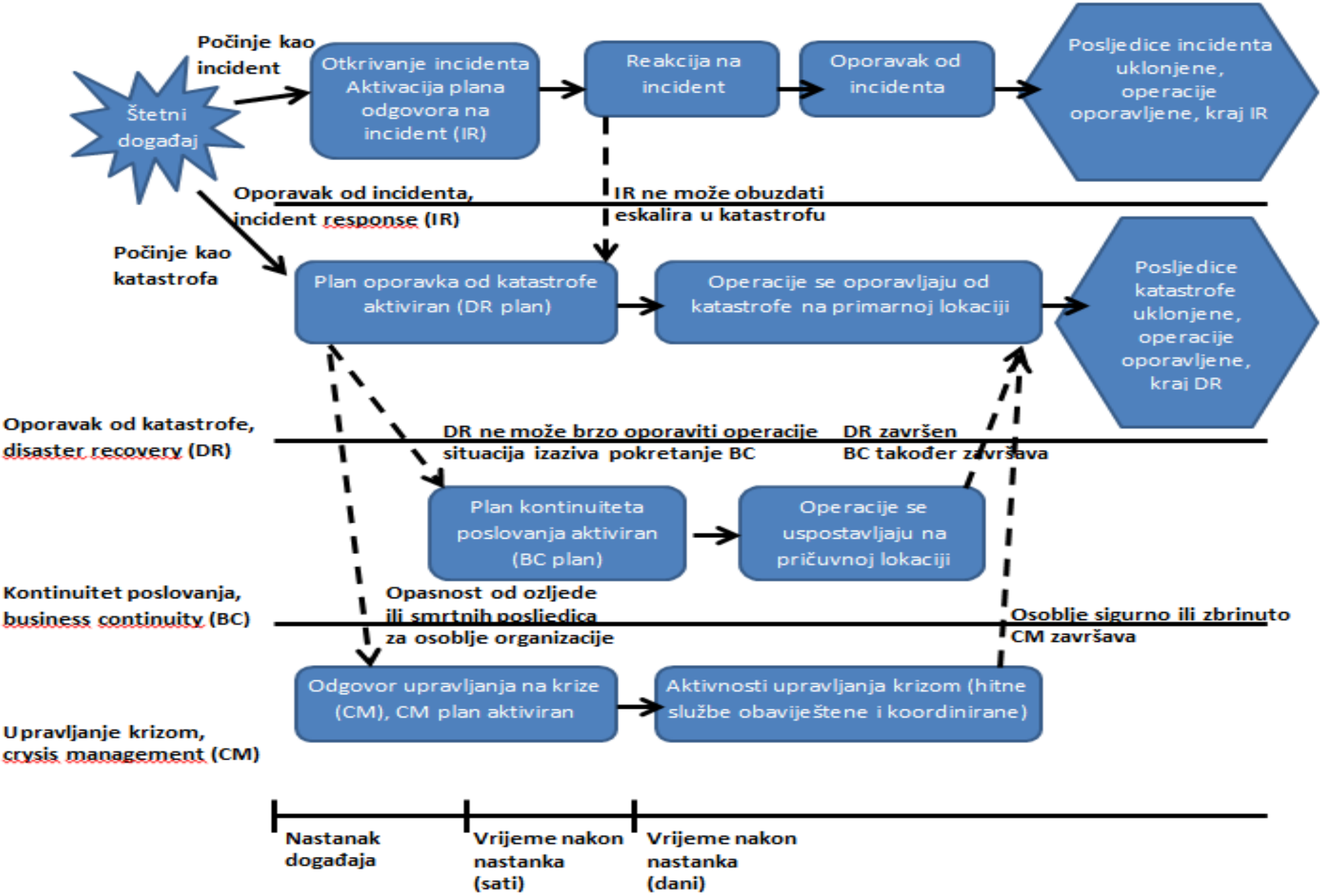


Planovi

- Plan za nepredviđene situacije (contingency plan)
  - Organizacija priprema kako bi se preduhitrili, reagirali i oporavili od događaja koji su prijetnja sigurnosti i informacijskoj imovini, te postupno doveli organizaciju u normalan tok rada
- Plan za odgovora na incident (Incident Response Plan – IR plan)
  - Prva, neposredna reakcija - ako situacija eskalira proširuje se na DRP i/ili BCP
- Plan oporavka od katastrofe (Disaster Recovery Plan – DR plan)
  - Obnavljanje sustava na originalnoj lokaciji nakon pojave katastrofe
- Plan kontinuiteta poslovanja (Business Continuity Plan – BC plan)
  - Konkurentno, održivost ključnih poslovnih funkcija, kad je šteta velika ili traje
  - Uspostavlja kritične poslovne funkcije na alternativnom mjestu - pričuvnoj lokaciji
- Dodatno, upravljanje krizom (Crisis Management – CM)
  - Bavljenje ozljedama, traumama i gubitkom života kao posljedicama katastrofe

Raspored planiranja nepredviđenih situacija




Počinje kao incident
Štetni događaj
Otkrivanje incidenta Aktivacija plana odgovora na incident (IR)
Reakcija na incident
Oporavak od incidenta
Posljedice incidenta uklonjene, operacije oporavljene, kraj IR
Oporavak od incidenta, incident response (IR)
IR ne može obuzdati eskalira u katastrofu
Počinje kao katastrofa
Plan oporavka od katastrofe aktiviran (DR plan)
Operacije se oporavljaju od katastrofe na primarnoj lokaciji
Posljedice katastrofe uklonjene, operacije oporavljene, kraj DR
Oporavak od katastrofe, disaster recovery (DR)
DR ne može brzo oporaviti operacije situacija izaziva pokretanje BC
DR završen BC također završava
Plan kontinuiteta poslovanja aktiviran (BC plan)
Operacije se uspostavljaju na pričuvnoj lokaciji
Kontinuitet poslovanja, business continuity (BC)
Opasnost od ozljede ili smrtnih posljedica za osoblje organizacije
Osoblje sigurno ili zbrinuto CM završava
Odgovor upravljanja na krize (CM), CM plan aktiviran
Aktivnosti upravljanja krizom (hitne službe obaviještene i koordinirane)
Upravljanje krizom, crysis management (CM)
Nastanak događaja
Vrijeme nakon nastanka (sati)
Vrijeme nakon nastanka (dani)

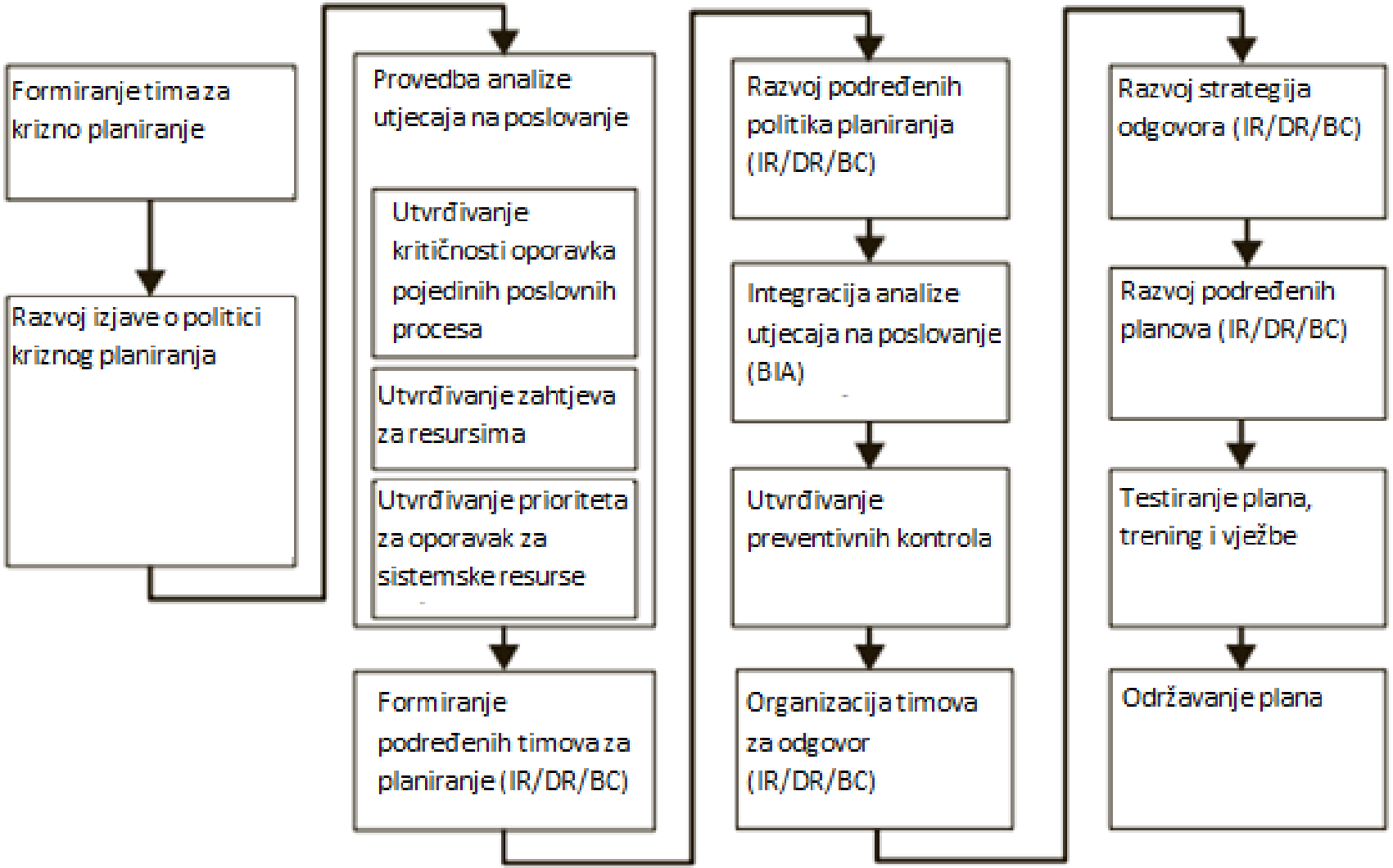
Tim za upravljanje planiranjem nepredviđenih situacija (CPMT)

- Tim za upravljanje planiranjem u nepredviđenim situacijama (CPMT)
  - Grupa viših menadžera i članova projekta organizirani da pro/vode sve napore CP
  - Formiranje tima i dodjela uloga prije nego započne planiranje
- Prvak, šampion (champion)
  - Viši rukovoditelj – potpora, promicanje, podržavanje
  - Idealno CIO (voditelj informatike) ili CEO (izvršni direktor)
- Voditelj projekta (project manager)
  - Srednji rukovoditelj ili CISO (chief information security officer)
- Članovi tima
  - Rukovoditelji ili predstavnici: poslovanje, IT, informacijska sigurnost

Cjelokupni proces planiranja za nepredviđene situacije

- Razvoj politike CP
  - Osiguranje autoriteta i smjernica za učinkovito planiranje
- Provedba BIA
  - Identifikacija i određivanje prioriteta ključnih IS za poslovne procese organizacije
- Određivanje preventivnih kontrola
  - Mjere za smanjenje učinaka poremećaja sustava i povećanje dostupnosti
- Izrada strategija za nepredviđene situacije
  - Strategije oporavka za brzi i učinkovit oporavak
- Razvoj plana za nepredviđene situacije
  - Detaljne preporuke i procedure za obnovu objekata prema zahtjevima za svaku organizacijsku cjelinu
- Osiguranje plana provjere, treninga i uvježbavanja
  - Provjera sposobnosti oporavka, trening i uvježbavanje osoblja
- Osiguranje održavanja plana
  - Periodičko ažuriranje sukladno poboljšanjima sustava i organizacijskim promjenama

Glavni koraci planiranja za nepredviđene situacije



Glavni koraci (2)

- Formiranje tima za krizno planiranje (CPMT)
  - Predstavnici upravljačke razine, poslovnih procesa te podređenih timova
- Razvoj izjave o politici CP
  - formalizirana politika – vodič za planiranje i ponašanje u slučaju nepredviđenih situacija
- Provedba analize utjecaja na poslovanje
  - Prepoznavanje poslovnih funkcija i IS kritičnih za poslovanje te određivanje njihovih prioriteta
- Formiranje podređenih timova
  - za planiranje koji će razviti IR, DR i BC planove, ne nužno istih za provođenje
- Razvoj podređenih politika
  - Timovi za područje IR, DR i BC
- Integracija analize utjecaja na poslovanje (BIA)
  - Svaki od podređenih timova treba procijeniti aspekte BIA važne za njihovo područje

Glavni koraci (3)

- Utvrđivanje preventivnih kontrola
  - Procjena protumjera i zaštitnih mjera za smanjenje rizika i posljedica štetnih događaja na podatke, poslovne procese i osoblje
- Organiziranje timova za odgovor
  - Navod vještina potrebnih za odgovor IR, DR i BC te odabir potrebnog osoblja
- Razvoj strategija odgovora (contingency strategies)
  - Pr. planovi izrade pričuvnih kopija i oporavka podataka, organizaciju alternativnih lokacija, …
- Razvoj podređenih planova
  - Aktivnosti za svako od područja (IR, DR, BC)
- Testiranje plana, trening i vježbe
  - Provjera učinkovitosti svakog od podređenih planova
- Održavanje plana
  - Periodička provjera, procjena plana te ažuriranje

Analiza utjecaja na poslovanje

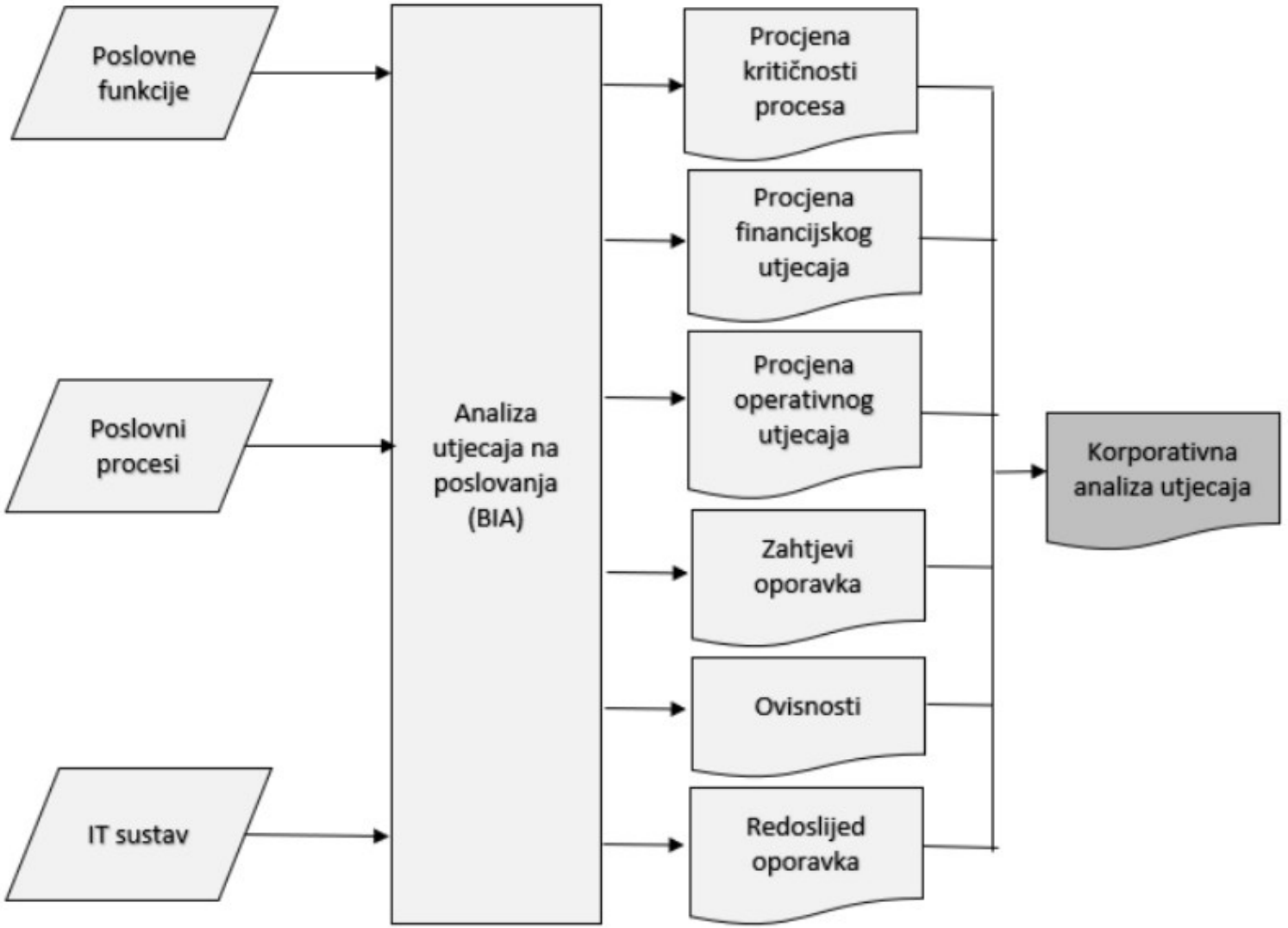
Analiza utjecaja na poslovanje

- Analiza utjecaja na poslovanje (Business Impact Analysis - BIA)
  - Ustanovljava organizacijske funkcije i njihove prioritete, kao i informacijske sustave koji podržavaju kritične poslovne procese
  - Upravljanje rizikom usmjerava se na prijetnje, ranjivosti i napade radi određivanja kontrola za zaštitu informacija
  - BIA pretpostavlja da kontrole mogu biti zaobiđene, neučinkovite
- Nastoji odgovoriti kako će to utjecati
  - **Doseg**: koje organizacijske cjeline i sustave obuhvatiti
  - **Plan**: podaci mogu biti obimni – uvažiti relevantne
  - **Ravnoteža**: objektivno-subjektivno, naglasak na znanju i iskustvu osoblja
  - **Cilj**: odrediti ključne donositelje odluka – informacije za donošenje
  - **Praćenje**: povremena provjera da vlasnici procesa i donositelji odluka podržavaju proces i rezultat BIA

Koraci BIA

- NIST SP 800-34 (National Institute of Standards and Technology)
  - Identifikacija ključnih poslovnih procesa i funkcija,
  - Utvrđivanje međuovisnosti informacijskih sustava i poslovnih procesa,
  - Utvrđivanje prioriteta i klasifikacija poslovnih procesa i funkcija,
  - Utvrđivanje utjecaja prekida poslovnih procesa na sveukupne poslovne operacije, s naglaskom na financijske i operativne utjecaje,
  - Utvrđivanje zahtijevanih vremena oporavka,
  - Utvrđivanje preduvjeta za oporavak poslovanja,
  - Utvrđivanje redoslijeda oporavka pojedinih procesa i funkcija.

Rezultat BIA: korporativna analiza utjecaja na poslovanje



Identifikacija poslovnih procesa i funkcija te procjena utjecaja

- **Kritične funkcije** (critical functions) - neophodne za poslovanje org. (core)
  - IT gledište - prekid ima ozbiljne/trajne sigurnosne, operativne i financijske učinke
  - Prihvatljivo vrijeme oporavka mjeri se satima
- **Bitne funkcije** (essential functions) - vrlo važne, ali ne ključne
  - Pr. isplata plaće zaposlenicima
  - Prihvatljivo vrijeme oporavka u IT segmentu – dan ili dva
- **Potrebne funkcije** (necessary functions)
  - Nedostupnost u duljem razdoblju može imati značajan učinak
  - Pr. E-pošta ili pristup Internetu, funkcije potpore poslovnim procesima
  - Prihvatljivo vrijeme oporavka mjeri se danima
- **Poželjne funkcije** (desirable functions) - mali učinak na poslovanje
  - Pomoćne funkcije koje su se razvile vremenom kao potpora poslovanju
  - Prekid može biti prilika za njihovu reviziju – može se ispostaviti da nisu potrebne
  - Prihvatljivo vrijeme oporavka – tjednima ili mjesecima

Zahtjevi oporavka

- Ciljana točka oporavka - RPO (Recovery Point Objective)
  - Vremenska tolerancija gubitka podataka, stanje povrata oporavkom pričuvne kopije podataka
  - Vrijeme između posljednjeg *backupa* i prekidnog događaja
    - Pr. tjedni backup + ispad u subotu → RPO = 1 tjedan

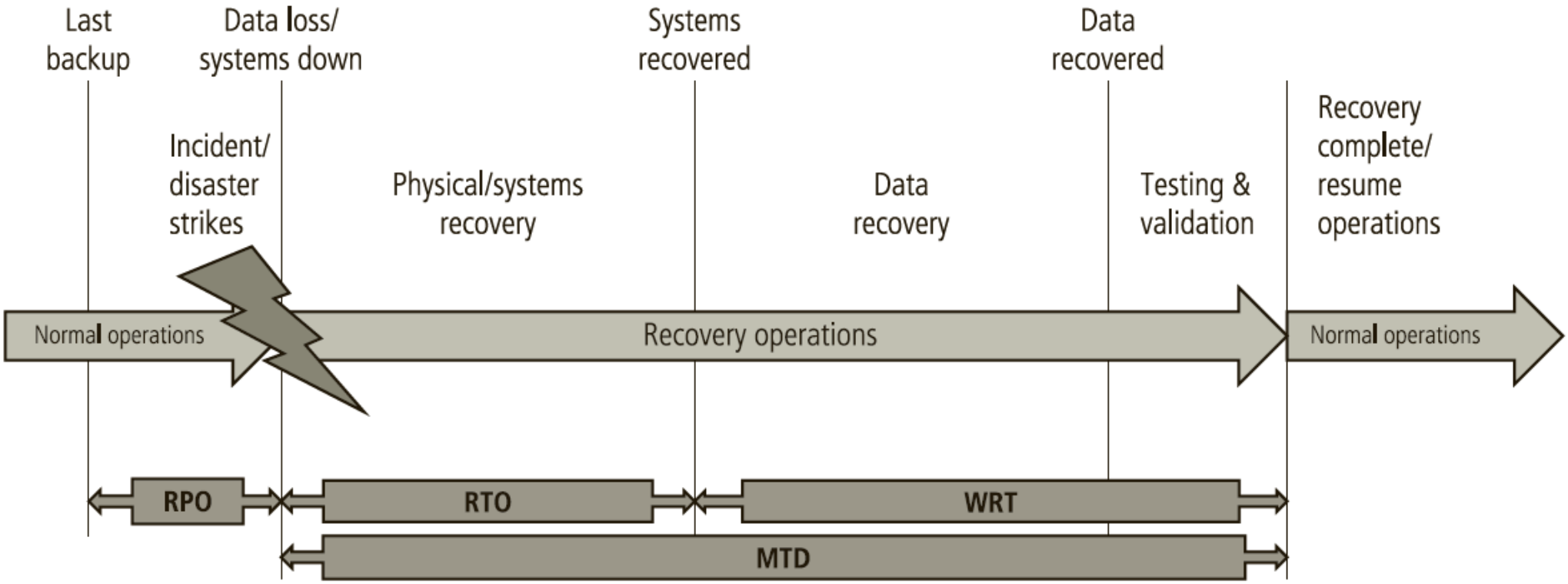
- Ciljano vrijeme oporavka - RTO (Recovery Time Objective)
  - Maksimalno vrijeme za oporavak resursa koji podržavaju misiju organizacije
    - Računalni sustavi, proizvodni uređaji, telekomunikacije, zgrade i radni prostor
  - Vrijeme između prekidnog događaja i oporavka sustava/resursa

- Vrijeme oporavka rada - WRT (Work Recovery Time)
  - Vrijeme potpunog oporavka poslovne funkcije nakon oporavka resursa
  - Obnova podataka (elektronički r*estore* i ručni unos) + testiranje i validacija

- Maksimalno prihvatljivo vrijeme ispada - MTD (Maximum Tolerable Downtime)
  - Maksimalno podnošljiv zastoj/ispad sustava mjeren trajanjem neraspoloživosti poslovnih procesa
  - Period između prekidnog događaja i početka normalnog poslovanja

  - MTD = RTO + WRT

Analiza i postavljanje prioriteta poslovnih procesa



Međuovisnosti poslovnih funkcija

- Kako će prekid određene poslovne funkcije utjecati na ostale i kada će to biti?
- Je li ta funkcija vezana za neke specifične resurse (određeni dobavljači, oprema)?
- Koje su ključne osobe za obavljanje te funkcije? Što kada su te osobe nedostupne?
- Kako se ta funkcija obavlja – kontinuirano, povremeno, na dnevnoj ili tjednoj bazi? Postoji li neko kritično vrijeme kada je neophodna za poslovanje?
- Koji su IT resursi neophodni za obavljanje te funkcije?
- Postoje li neke ručne, zaobilazne procedure kojima se ona može izvršavati i ako informacijski sustav nije dostupan?

Izvješće o analizi utjecaja

- Ključni procesi i funkcije,
- Međuovisnosti procesa i IT resursa,
- Kritičnost odnosno razina utjecaja na poslovanje,
- Ključne uloge i odgovornosti osoba zaduženih za njihovu provedbu,
- Zahtijevana vremena oporavka,
- Financijski, operativni, pravni, personalni učinci nedostupnosti,
- Ručne procedure za nastavak poslovanja u slučaju nedostupnosti.

Odgovor na incident

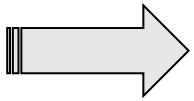
Planiranje odgovora na incidente (IRP)

- Identifikacija i klasifikacija incidenata te odgovarajućih odgovora

- Tim za planiranje odgovora na incident (IR team)
  - Razvija planove za odgovor na incident

- Tim za odgovor na incident
  - Computer Security Incident Response Team (CSIRT)
  - Izvodi planove, kao reakciju na incident

- Faze odgovora na incident
  - Planiranje (planning)
  - Detekcija (detection)
  - Reakcija (reaction)
  - Oporavak (recovery)



Uspostava tima za odgovor na incidente

- Srodni pojmovi

- Computer Security Incident Response Team (CSIRT)
  - usluga odgovorna za zaprimanje, pregled i odgovor na prijavu incidenata računalne sigurnosti – organizacijsko tijelo, ali može biti i vanjsko

- Tim za odgovor na incidente informacijske sigurnosti
  - Information Security Incident Response Team (ISIRT)
  - prema normi ISO/IEC 27035:2011 (više ne vrijedi)
  - tim odgovarajuće vještih i pouzdanih članova organizacije koji tijekom svog životnog ciklusa rješavaju incidente informacijske sigurnosti

- Computer Emergency Response (CERT)
  - tim za IKT incidente, organizacijski, češće nacionalni, gdje može biti i drukčije nazvan
  - Pr. https://www.cert.hr/ , https://www.cert.hr/csirt_specifikacija/

Politika odgovora na incidente

- NIST 800-61, Rev. 2, The Computer Security Incident Handling Guide
  - Izjava o svrsi i ciljevima politike
  - Doseg – na koga se što odnosi te u kojim okolnostima
  - Definicija incidenata i povezanih pojmova
  - Organizacijska struktura, definicija uloga, odgovornosti i ovlasti
    - Zapljena ili isključivanje opreme, nadzor sumnjivih aktivnosti, prijava počinitelja
    - Dijeljenje informacija (što, tko, kada, kako)
    - Postupak eskalacije
  - Postavljanje prioriteta ili ocjene ozbiljnosti incidenata
  - Mjerenje učinaka (kontrola pristupa, sigurnosne stijene, DNS, …)
  - Izvještavanje i formulari

Planiranje odgovora na incident

- Pretpostavka je da postoji CSIRT
  - Kompetencije, dežurstva, …
- Format i sadržaj
  - Organizirane upute o procedurama postupanja
  - … za vrijeme i nakon incidenta
- Smještaj – zaštita IR plana
  - Pri ruci, ali tako da ih napadač ne otkrije
  - Fizički registratori blizu administratorskih stanica, ormari, šifrirane datoteke
- Testiranje
  - Kontrolne liste, strukturirani prohod (walk-through), simulacija, potpuni prekid

- The more you sweat in training, the less you bleed in combat.
- Training and preparation hurt.
- Lead from the front, not the rear.
- You don't have to like it, just do it.
- Keep it simple.
- Never assume.
- You are paid for your results, not your methods.

Detekcija incidenta

- Indikatori mogućih incidenata
  - Nepoznate datoteke
  - Nepoznati procesi
  - Neuobičajeno trošenje računalnih resursa
  - Neuobičajen pad sustava

- Indikatori vjerojatnih incidenata
  - Aktivnosti u neuobičajena vremena (mrežni promet ili pristup datotekama „kada ih nitko ne koristi“)
  - Pojava novih vjerodajnica
  - Napadi prijavljeni od strane korisnika
  - Notifikacije IDPS (Intrusion Detection / Prevention System)

Detekcija incidenta (2)

- Indikatori izvjesnih incidenata
  - Korištenje neaktivnih vjerodajnica
  - Izmjene dnevničkih zapisa (u odnosu na rezervnu kopiju)
  - Prisustvo hakerskih alata
  - Dojava partnera ili parnjaka (partner, *peer*)
  - Poruka hakera – „gotcha“ na web stranici ili email poruka sa „sigurnog“ računa

- Drugi indikatori
  - Gubitak raspoloživosti - nedostupan sustav
  - Gubitak integriteta - korumpirane datoteke ili podaci
  - Gubitak povjerljivosti - obavijest o curenju podataka ili otkrivanje podataka za koje se mislilo da su zaštićeni
  - Kršenje politike – događaji u suprotnosti s org. politikama sigurnosti
  - Kršenje zakona – prekršen je zakon u čemu su sudjelovala org. sredstva

Reakcija – ključni pojmovi

- Poruka upozorenja (alert message)
  - Opis incidenta s dovoljno informacija
  - Da svaka osoba zna koji dio IR plana provesti bez da uspori obavješćivanje
- Popis upozorenja (alert roster)
  - Kontakti koje treba obavijestiti o događaju incidenta
  - Hijerarhijski popis (hierarchical roster)
    - Popis upozorenja u kojem prva osoba poziva nekoliko drugih, a one dalje
    - brže ali nepreciznije
  - Slijedni popis (sequential roster)
    - Popis upozorenja u kojem jedna osoba poziva svaku na popisu
    - točnije ali dugotrajnije

Reakcija - postupak

- Pomoćna služba (help desk), korisnik ili administrator sustava
  - Pozivaju „prave ljude” s popisa upozorenja
- Dokumentiranje incidenta
  - Tko, što, kada, gdje, zašto i kako
  - Studijski slučaj, učenje
  - Dokaz za ispravno postupanje
  - Podloga za simulacije u budućnosti
- Strategije suzbijanja incidenata i povrata kontrole
  - Filtriranje poruka, blokiranje priključnica, onesposobljavanje vjerodajnica, rekonfiguriranje sig. stijene, privremeno zaustavljanje servisa i procesa

Oporavak od incidenta

- Ulaganje napora po prioritetima – slijeđenjem plana
- Procjena štete
  - Trenutno, danima, tjednima
  - Procjena sustava i pohrane podataka
  - Proučavanje dnevnika (log), računalna forenzika, prikupljanje dokaza
- Oporavak
  - Identifikacija ranjivosti
  - Instalacija, zamjena, nadogradnja zaštite
  - Oporavak podataka, usluga, procesa
  - Kontinuirano praćenje/nadzor sustava
  - Obnavljanje povjerenja
- Naknadna revizija (After Action Review - AAR)

Oporavak od katastrofe

Katastrofa

- neželjeni i neočekivani štetni događaj koji organizaciji
- onemogućuje obavljanje kritičnih poslovnih funkcija
- kroz neodređeni vremenski period i
- rezultira velikom štetom (ne samo financijskom) za njezino poslovanje

- Neki primjeri
  - nedostupnost glavne lokacije organizacije zbog prirodne katastrofe ili požara,
  - nedostupnost IT infrastrukture na glavnoj lokaciji zbog kvara hardvera ili softvera većih razmjera,
  - nedostupnost ključnih djelatnika organizacije zbog epidemije,
  - dugotrajni prekid isporuke električne energije,
  - prekid ključnih usluga dobavljača

Sadržaj plana oporavka od katastrofe (DR plan)

- Popis IT sredstava
  - inventura hardvera, sustava i aplikacija
- Procjena rizika
  - za svaki ključni IS; vjerojatnost, posljedice
- Klasifikacija važnosti
  - kritični, ostali
- RPO i RTO
- Popis aktivnosti – procedure uspostave nastavka poslovanja
  - Kratkoročne – osnovne funkcionalnosti
  - Dugoročne – poslovanje se vraća u uobičajeno stanje

Aktivnosti oporavka

- Oporavak hardvera
  - Zamjena komponenti na glavnoj ili pričuvnoj lokaciji
  - Poslužitelji, mrežna oprema, vatrozid, IP/DS
- Oporavak operacijskih sustava
  - OS i glavni servisi (npr. DNS, AD)
- Oporavak baza podataka i arhivskih zapisa
- Oporavak spremišta podataka
  - *Storage*, pričuvni hardver (Storage Area Network – SAN)
- Oporavak aplikacija
  - Podaci, sinkronizacija s pričuvnom lokacijom, provjera
- Testiranje procedura oporavka

Razine oporavka od katastrofe (IBM, 2007)

- Razina 0 – bez pohrane podataka na pričuvnoj lokaciji
  - Podatci se ne pohranjuju na drugoj lokaciji
  - Oporavak je moguć samo korištenjem sustava na primarnoj lokaciji

- Razina 1 – Izrada pričuvne kopije podataka s hladnom lokacijom
  - Podatci se pohranjuju na diskove/trake i fizički šalju na pričuvnu lokaciju
    - Pickup Truck Access Method (PTAM)
  - Pričuvna hladna lokacija (cold site)
    - samo osnovna infrastruktura poput namještaja, napajanja, mrežnih ormara i utičnica
    - uspostava HW i SW, pa vraćanje pričuvnih kopija podataka
  - Jeftino rješenje, nastavak rada obično moguć tek nakon nekoliko dana

Razine oporavka od katastrofe (BC tier 2 - 4)

- Razina 2 – Izrada pričuvne kopije podataka s vrućom lokacijom
  - Pričuvne kopije se fizički šalju na pričuvnu lokaciju - PTAM
  - Pričuvna vruća lokacija (host site)
    - na kojoj je instaliran i aktivan pričuvni sustav s odgovarajućim HW i SW, pa vraćanje podataka
  - Skuplje rješenje, nastavak rada unutar 24 sata

- Razina 3 – Elektronička pohrana (Electronic vaulting)
  - BC2 + Kritični podaci elektronički na pričuvnu lokaciju (remote backup service)
  - Efikasnije, nastavak rada za desetak sati

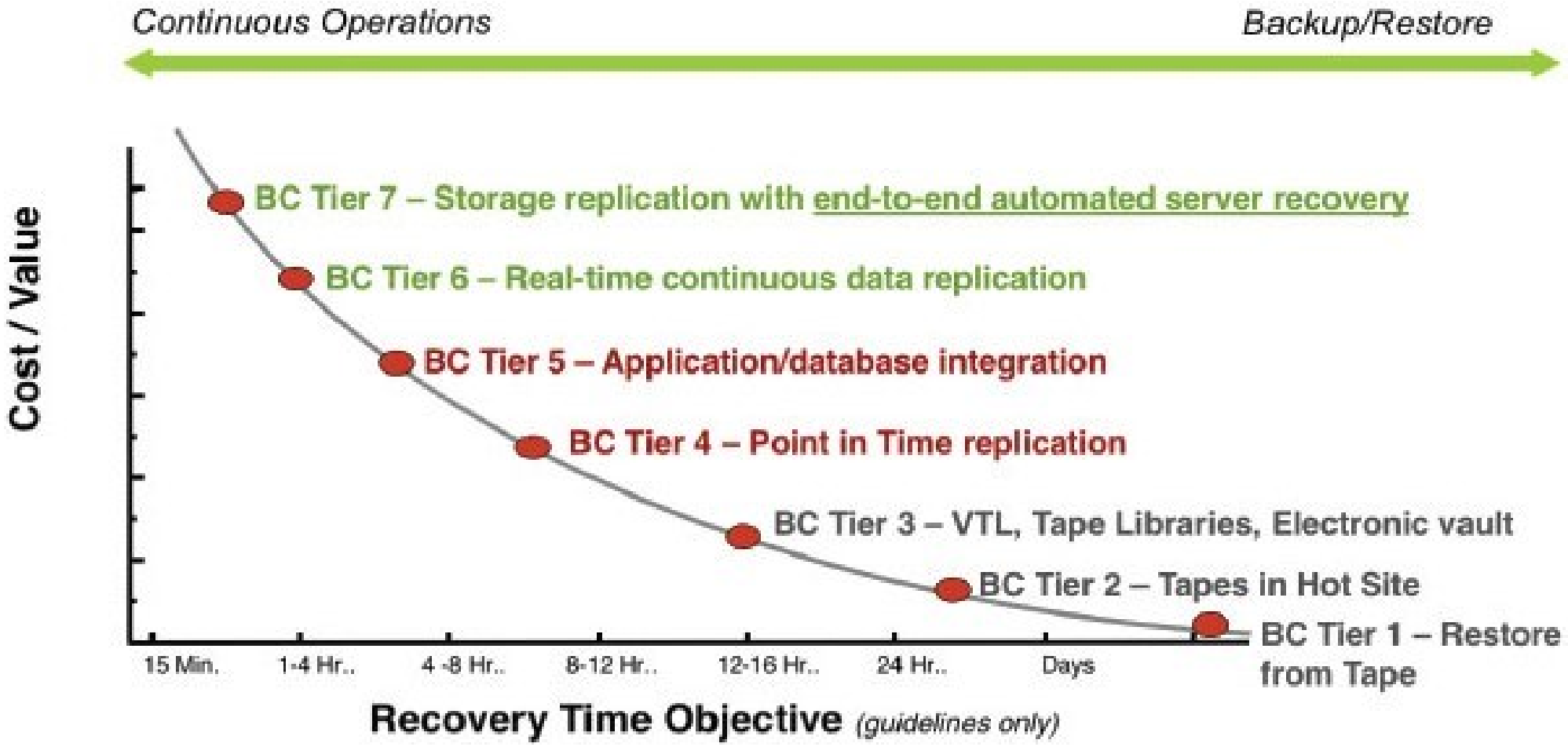
- Razina 4 – Aktivna pričuvna lokacija
  - Svi podatci periodički elektronički kopirani na pričuvnu lokaciju (point-in-time copies)
    - *Batch/Online Database Shadowing and Journaling, Global Copy, FlashCopy, …*
  - Gubitak podataka do nekoliko sati

Razine oporavka od katastrofe (BC tier 5 - 7)

- Razina 5 – Integritet transakcija
  - Aplikacijski podatci i podatci iz BP se na transakcijskoj razini preslikavaju na diskove na pričuvnoj lokaciji (two-phase commit, remote replication, …)
  - Oporavak ovisan o korištenom softveru
- Razina 6 – Minimalni ili nikakav gubitak podataka
  - Svi podatci (neovisno o aplikaciji) se „trenutno” kopiraju s primarne na pričuvnu
  - Elektronički (real-time storage mirroring, server mirroring), najčešće zrcaljenjem diska (disk-mirroring)
- Razina 7 – Potpuno automatizirano rješenje
  - Nadgradnja razine 6 pri kojoj u slučaju katastrofe IS automatski nastavlja raditi na hardverskoj infrastrukturi, aplikacijama i podatcima koji se nalaze na pričuvnoj lokaciji bez ikakvog prekida ili gubitka podataka

Razine oporavka i kontinuitet poslovanja

- BC1-3 *backup/restore*, BC4-5 brzi oporavak, BC6-7 kontinuirana dostupnost



Varijante pričuvne lokacije

- Cold – infrastruktura, Warm – bez aplikacija, Hot – potpuna konfiguracija

Hladna lokacija

- malo ili bez opreme
- nema mrežne veze
- nije spremna za automatsko preuzimanje
- nema sinkronizacije podataka
-velik rizik gubitka podataka
- jeftino

Topla lokacija

- djelomično dostupna oprema
- mrežna veza aktivna
- preuzimanje unutar nekoliko sati
- dnevna sinkronizacija
-mali gubitak podataka
- financijski isplativo

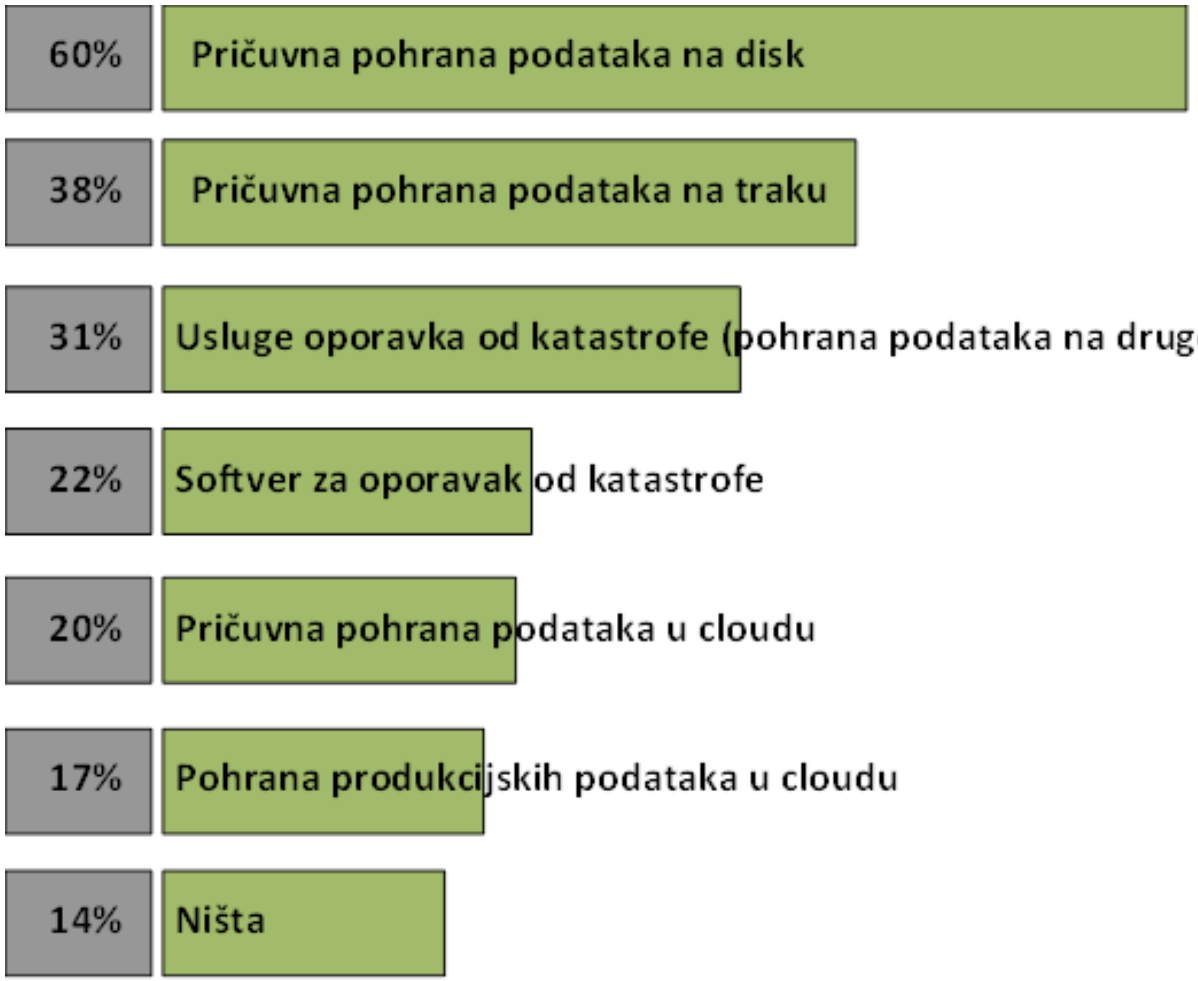
Vruća lokacija

- potpuno dostupna oprema
- mrežna veza aktivna
- preuzimanje unutar nekoliko minuta
- gotovo trenutna sinkronizacija
- bez gubitka podataka
- skupo

Procedure za prelazak s primarne na pričuvnu lokaciju i obrnuto

- ***Failover* (activation)**
  - Automatski nastavak rada na pričuvnom poslužitelju, računalnoj ili mrežnoj komponenti u slučaju kvara na primarnom P/RK/MK
  - Pravi automatizirani *failover* moguć samo na razini BC7
- ***Switchover* (role switch)**
  - Kontrolirana zamjena uloga, najčešće ručno u planirano vrijeme
  - Priprema za održavanje – instalacija zakrpa, nadogradnji, …
  - Također za prelazak na pričuvnu kada je *failover* prekompliciran ili preskup
- ***Failback***
  - Nakon osposobljavanja sustava na primarnoj lokaciji
  - Vraćanje promjena u podacima i aplikacijama
  - U idealnom slučaju (BC7) automatski
  - U praksi uz manji ili veći gubitak podataka, ovisno o rješenju

Alati i tehnologije za oporavak od katastrofe



- DRaaS - DR as a Service
- BaaS - Backup as a Service
  - IBM BaaS
  - Veeam Cloud Connect Replication
  - MS Azure Site Recovery
- DR Tools
  - Zerto
  - Carbonite
  - Arcserve
  - Veritas
  - Datto
- Virtualizacija
  - VMware ESX, ESXi
  - MS Hyper-V

https://www.softwaretestinghelp.com/best-disaster-recovery-services-and-software-tools/

Kontinuitet poslovanja

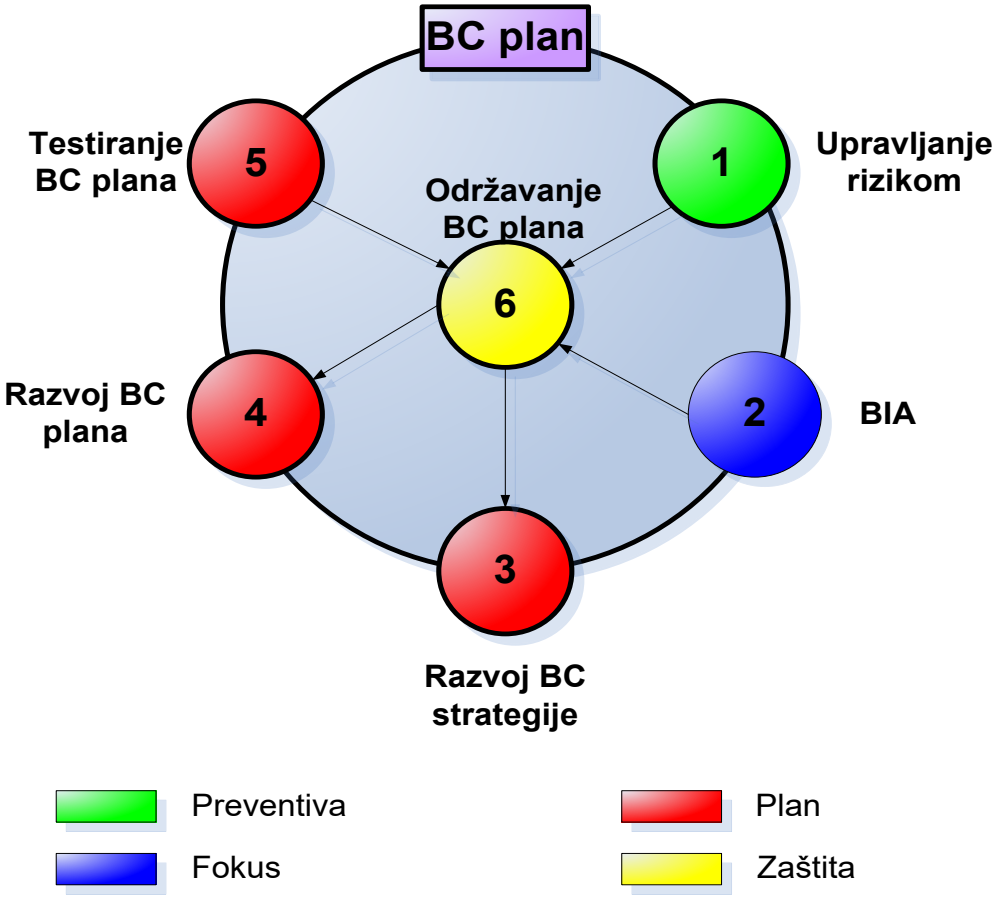
Planiranje kontinuiteta poslovanja

- Napori organizacije da nastavi s kritičnim funkcijama u slučaju ispada primarne lokacije
  - Više rukovodstvo – razvoj i implementacija BC politike, plana te timova

- Uspostava sustava upravljanja kontinuitetom poslovanja (Business Continuity Management System - BCMS), prema normi:
  - ISO 22301 Security and resilience — Business continuity management systems — Requirements
  - ISO 22313 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

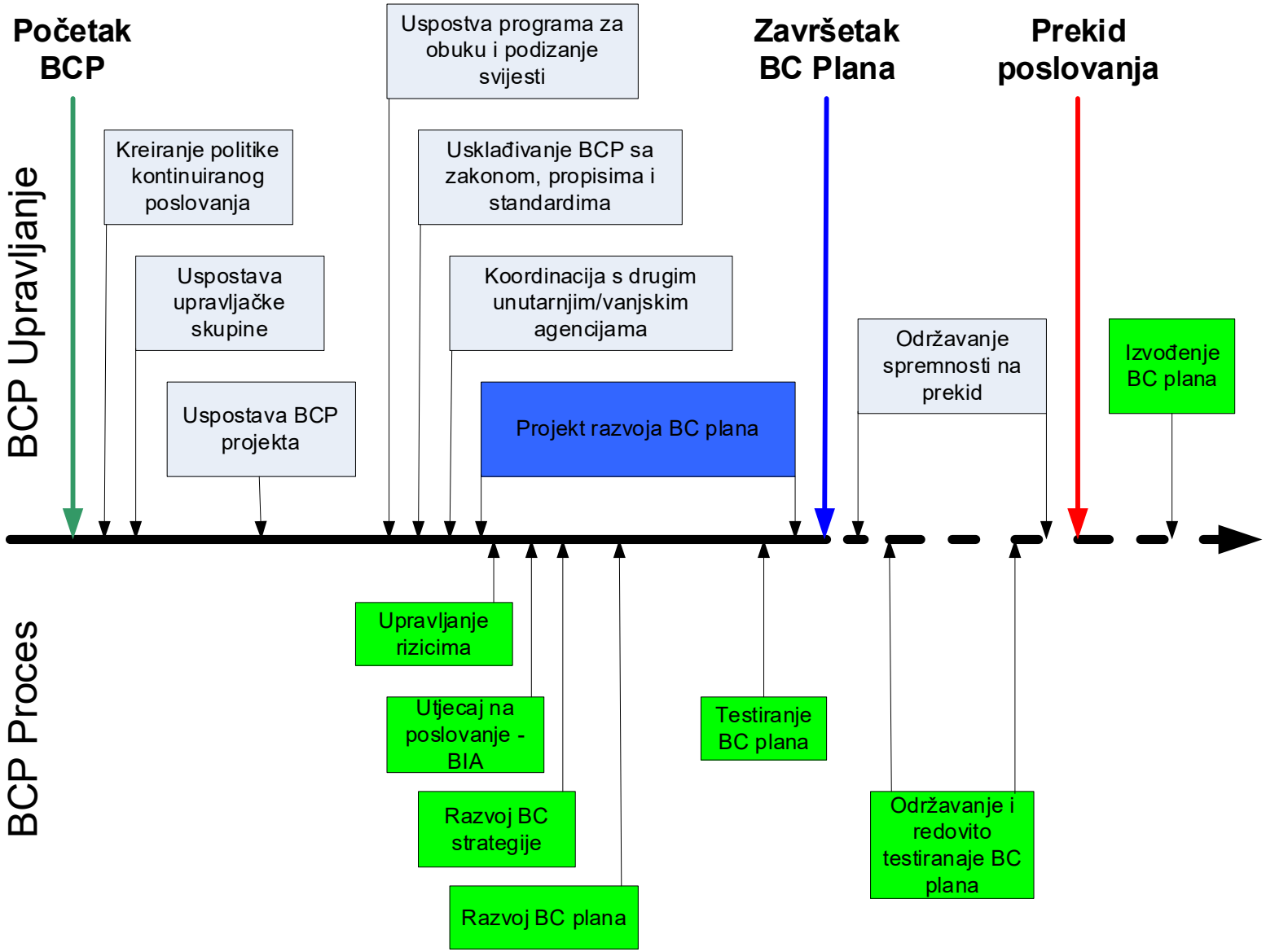
Proces planiranja kontinuiteta poslovanja

- Proces slijedi četiri ključna načela: *Fokus, Preventiva, Plan, Zaštita*
  - koji se implementiraju u BC programu kroz proces planiranja u šest koraka:



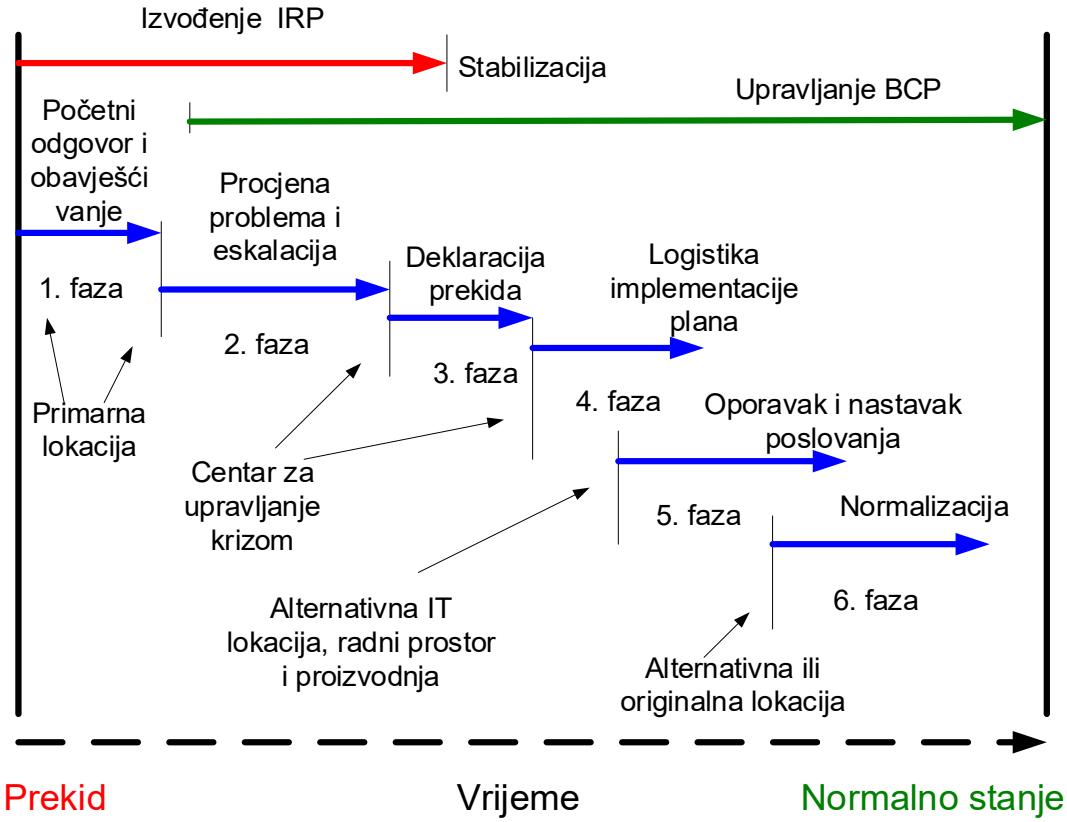
Planiranje kontinuiteta poslovanja

- Upravljanje rizikom
  - Procjena prijetnji i rizika za kontinuitet poslovanja, kontrola rizika
- Analiza posljedica na poslovanje (BIA)
  - Identifikacija ključnih poslovnih funkcija i procesa, analiza mogućih posljedica
  - Identifikacija zahtjeva za oporavak nakon pojave katastrofe
- Razvoj strategije kontinuiranog poslovanja
  - Ocjena zahtjeva za oporavak prekinutih ključnih poslovnih procesa.
  - Ustanovljavanje rješenja koja zadovoljavaju zahtjeve, odabir isplativih rješenja
- Razvoj BC plana
  - Zaštita ključnih procesa i sredstava od različitih prijetnji i rizika
  - Oporavak ključnih poslovnih procesa i resursa na siguran i vremenski prihvatljiv način
- Testiranje BC plana
  - Testiranje sposobnosti i učinkovitosti tima za oporavak
  - Testiranje sposobnosti i učinkovitosti dobavljača robe i usluga
- Održavanje BC plana


Početak BCP
Uspostva programa za obuku i podizanje svijesti
Završetak BC Plana
Prekid poslovanja
BCP Upravljanje
Kreiranje politike kontinuiranog poslovanja
Usklađivanje BCP sa zakonom, propisima i standardima
Uspostava upravljačke skupine
Koordinacija s drugim unutarnjim/vanjskim agencijama
Održavanje spremnosti na prekid
Izvođenje BC plana
Uspostava BCP projekta
Projekt razvoja BC plana
BCP Proces
Upravljanje rizicima
Utjecaj na poslovanje - BIA
Testiranje BC plana
Razvoj BC strategije
Održavanje i redovito testiranje BC plana
Razvoj BC plana

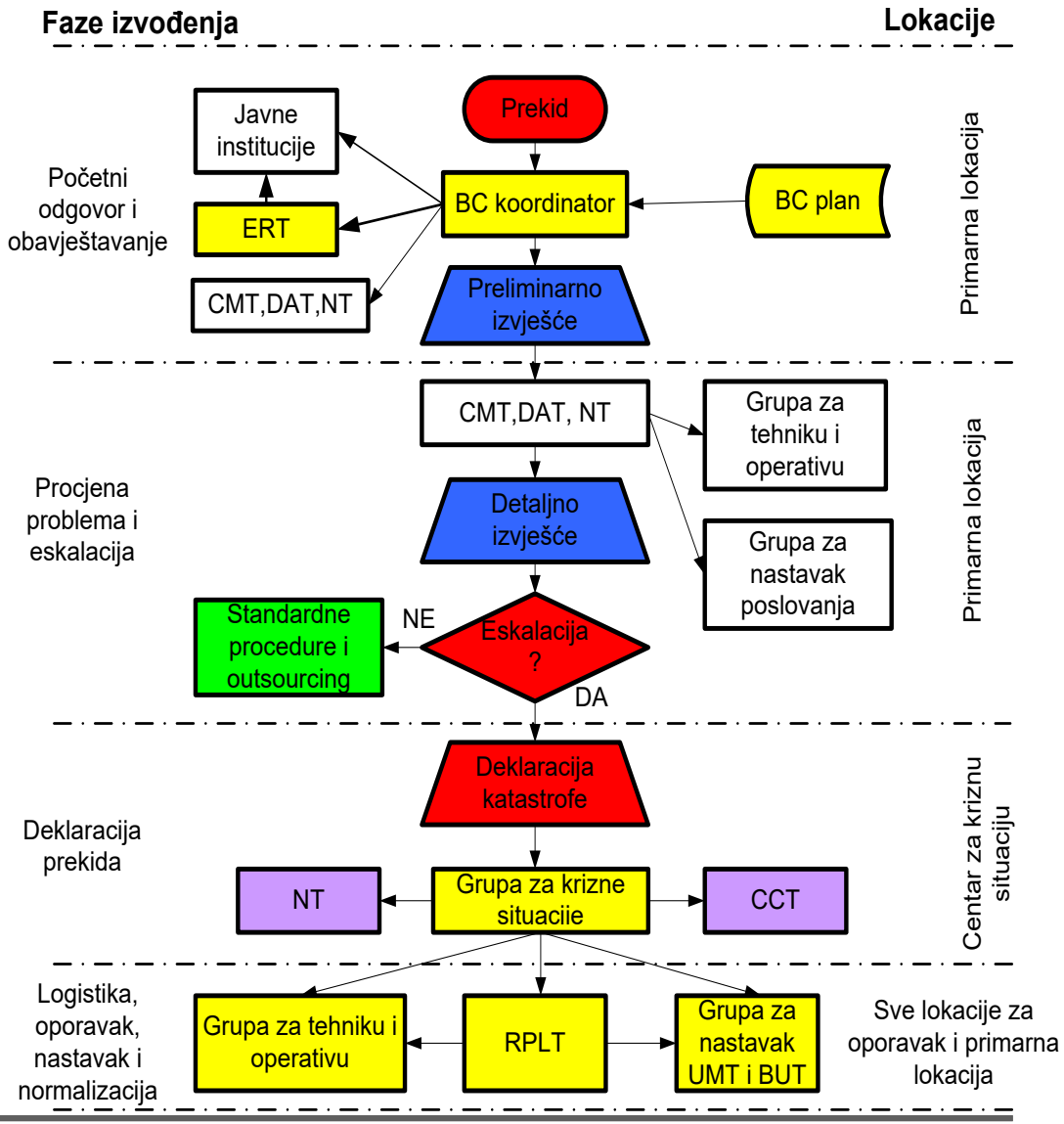
Izvođenje plana BC

- Početni odgovor i obavijest
  - preliminarno izvješće o problemu
- Procjena problema i eskalacija
  - detaljno izvješće o problemu
- Izjava o katastrofi / prekidnom događaju
  - proglašenje katastrofe / prekidnog događaja
- Implementacija plana logistike
  - mobilizacija timova, backup medija, kritičnih resursa i uređaja
- Oporavak i nastavak poslovanja
  - oporavak kritičnih IT i ne-IT resursa i nastavak procesa
- Normalizacija
  - operativni status kakav je bio prije pojave prekida



Uloge i odgovornosti pri izvođenju plana BC

- ERT – Emergency Response Team
- CMT – Crisis Management Team
- DAT – Data Team
- NT – Notification Team
- CCT – Command & Control Team
- RPLT – Resource Procurement and Logistics Team
- UMT – User Management Team
- BUT – Business Unit Team



Reference

- ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
  - Application of ISO/IEC 27002 to information and communication technology readiness for business continuity
- ISO/IEC 27035:2016+ — Information technology — Security techniques — Information security incident management
- NIST Special Publication (SP) 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems
- NIST 800-61, Rev. 2, The Computer Security Incident Handling Guide
- ISO 22301 Security and resilience — Business continuity management systems — Requirements
- ISO 22313 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301