Protection and security of information systems

Business continuity planning for unforeseen cases

prof. Ph.D. Krešimir Fertalj

University of Zagreb

Faculty of Electrical Engineering and Computing

Creative Commons

- **you are free to:**
  - **share**—reproduce, distribute and communicate the work to the public
  - **remix**—rework the work
- **under the following conditions:**
  - **appointment**. You must acknowledge and attribute the authorship of the work in a manner specified by the author or licensor (but not in a manner that suggests that you or your use of their work has their direct endorsement).
  - **non-commercial**. You may not use this work for commercial purposes.
  - **shares under the same conditions**. If you modify, transform, or create using this work, you may distribute the adaptation only under a license that is the same or similar to this one.

In the case of further use or distribution, you must make clear to others the license terms of this work. The best way to do this is to link to this website.

Any of the above conditions may be waived with the permission of the copyright holder.

Nothing in this license infringes or limits the author's moral rights.

The text of the license was taken from http://creativecommons.org/.

basic terms

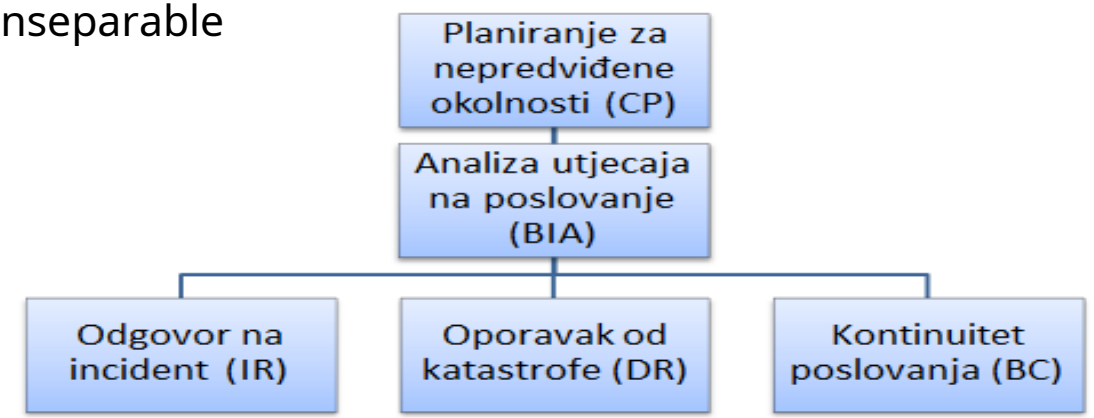
- adverse event
  - An event with negative consequences that could threaten the organization's resources or operations - attack, sabotage, earthquake, flood, fire, gas leak, radiation, ...
  - A possible candidate for the incident

- Incident
  - A harmful event that may result in the loss of information assets, but does not currently threaten the viability of the entire organization
  - A clearly identified attack on an information asset that may compromise its confidentiality, integrity, or availability

- disaster
  - A harmful event that could threaten the sustainability of the entire organization
  - It escalates from an incident or is declared immediately

Contingency planning

- Contingency planning (CP)
  - senior management determines what happens when an adverse event becomes an incident or disaster
- Elements
  - Business Impact Analysis (BIA)
  - Incident Response (IR), Disaster Recovery (DR) and Business Continuity (BC) planning
    - Business Resumption Planning (BRP) = DRP + BCP
    - Plans DR and BC are considered inseparable



Plans

- Contingency plan
  - The organization prepares to prevent, react and recover from events that are a threat to security and information assets, and gradually bring the organization to a normal work flow

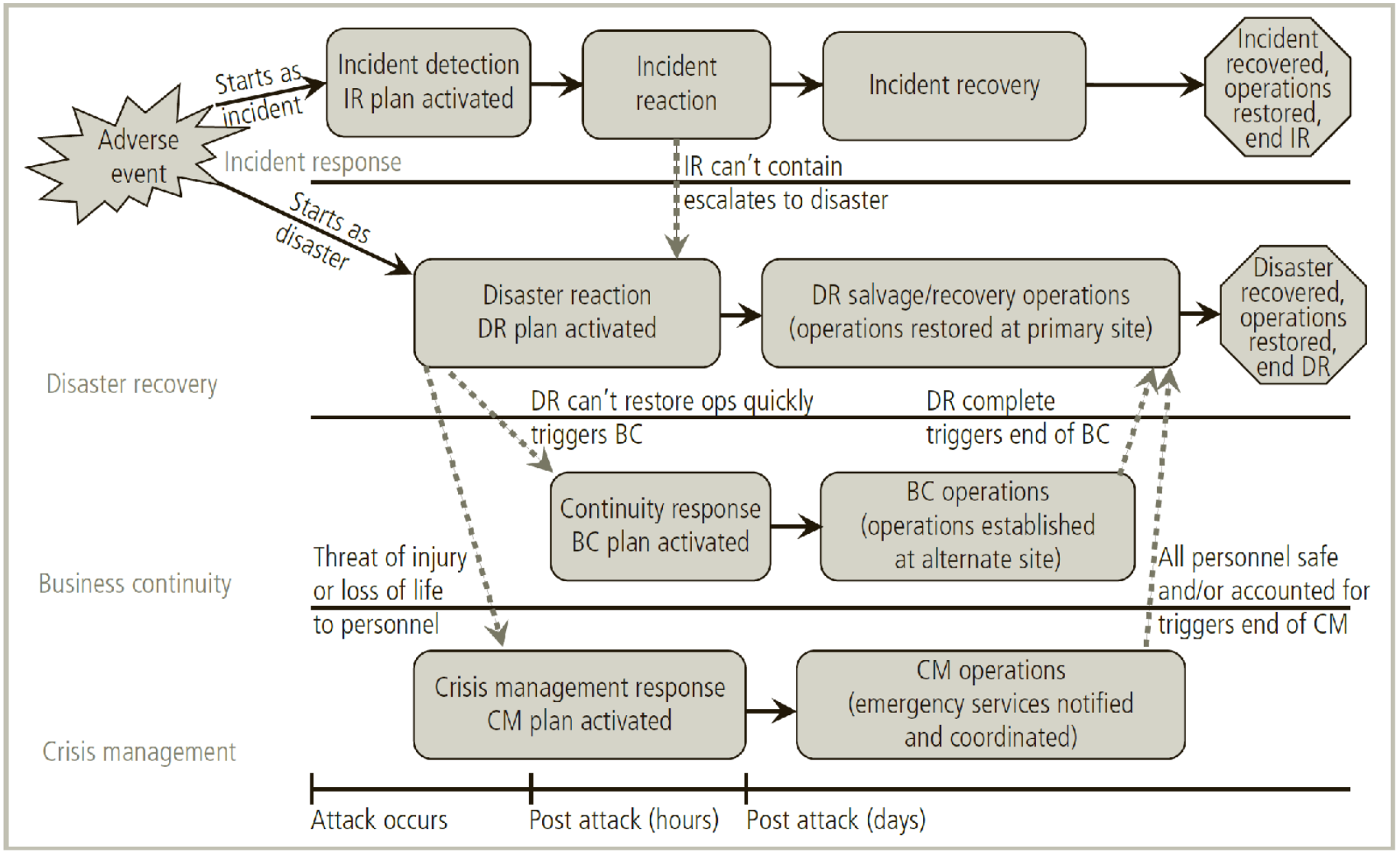
- Incident Response Plan (IR plan)
  - The first, immediate reaction - if the situation escalates, it is extended to DRP and/or BCP

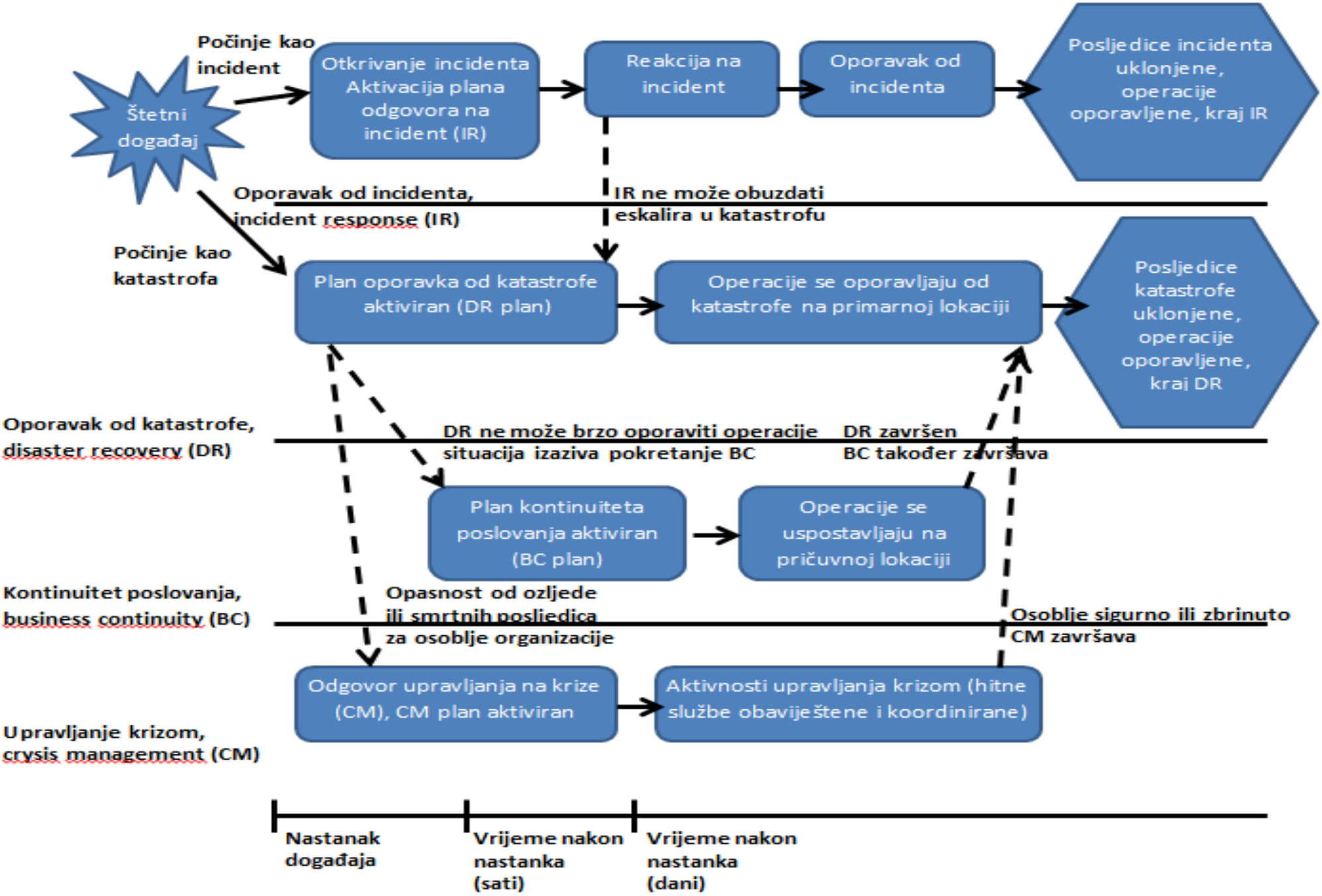
- Disaster Recovery Plan (DR plan)
  - System Restorein the original locationafter the occurrence of a disaster

- Business Continuity Plan (BC plan)
  - Competitively, the sustainability of key business functions, when the damage is large or ongoing
  - Establishes critical business functionsat an alternative location - reserve location

- In addition, crisis management (Crisis Management – CM)
  - Dealing with injuries, trauma and loss of life as a result of a disaster

Contingency planning schedule




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)

Contingency Planning Management Team (CPMT)

- Contingency Planning Management Team (CPMT)
  - A group of senior managers and project members organized to implement/lead all CP efforts
  - Forming a team and assigning roles before planning begins

- champion
  - Senior manager - support, promotion, support
  - Ideally CIO (head of information technology) or CEO (executive director)

- Project manager
  - Middle manager or CISO (chief information security officer)

- Team members
  - Managers or representatives: business, IT, information security

The entire contingency planning process

- Development of CP policy
  - Providing authority and guidance for effective planning

- Implementation of BIA
  - Identification and prioritization of key IS for the organization's business processes

- Determination of preventive controls
  - Measures to reduce the effects of system disruptions and increase availability

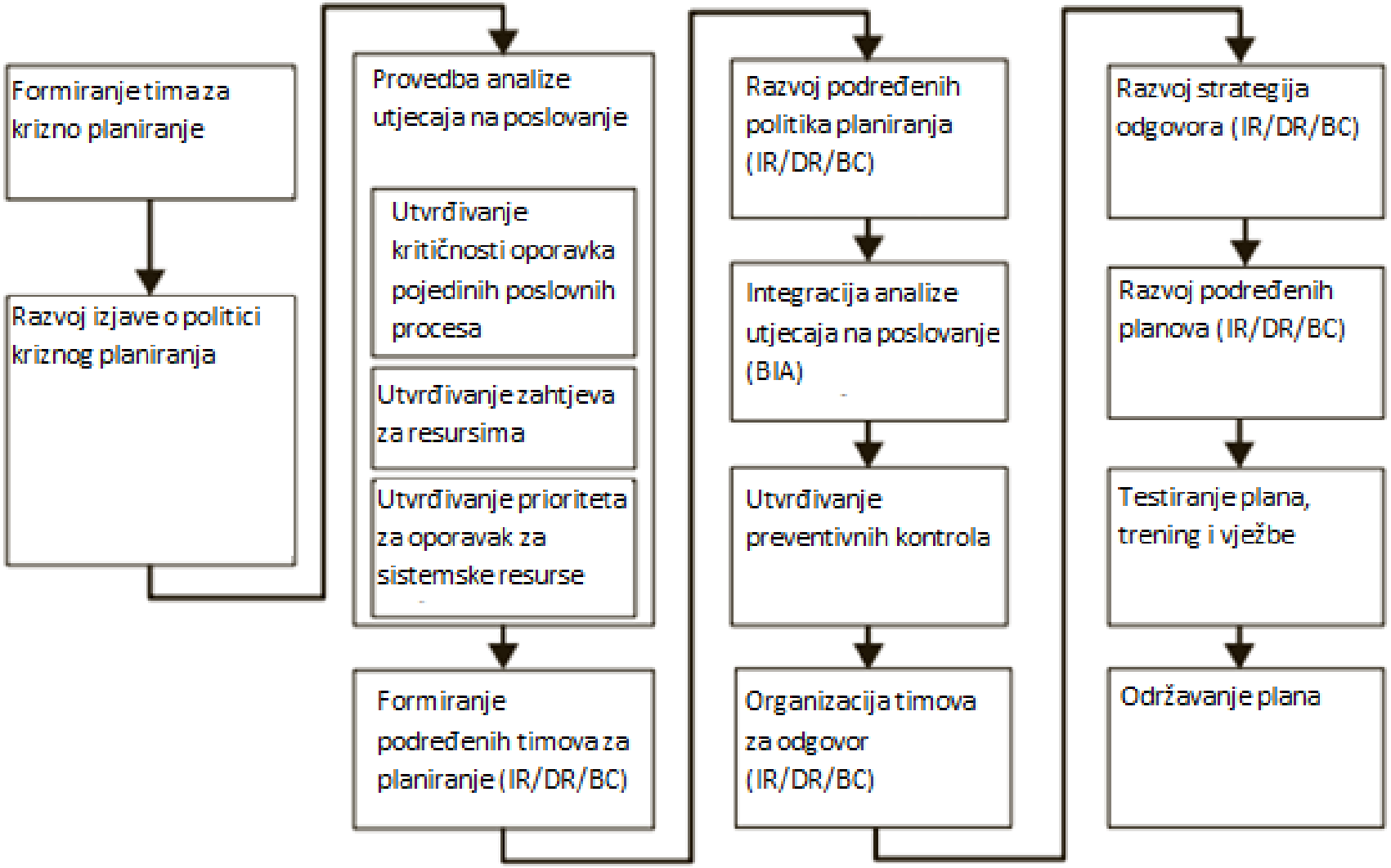
- Developing strategies for unforeseen situations
  - Recovery strategies for quick and effective recovery

- Development of a contingency plan
  - Detailed recommendations and procedures for the renovation of facilities according to the requirements for each organizational unit

- Ensuring a plan of verification, training and exercise
  - Recovery ability testing, training and staff training

- Plan maintenance insurance
  - Periodic updating in accordance with system improvements and organizational changes

The main steps of contingency planning



Main steps (2)

- Formation of the Crisis Planning Team (CPMT)
  - Representatives of the management level, business processes and subordinate teams
- Development of CP policy statement
  - formalized policy – a guide to contingency planning and behaviour
- Implementation of an analysis of the impact on business
  - Identification of business functions and IS critical for business and determination of their priorities
- Formation of subordinate teams
  - for planning that will develop IR, DR and BC plans, not necessarily for implementation
- Development of subordinate policies
  - IR, DR and BC area teams
- Integration of Business Impact Analysis (BIA)
  - Each of the subordinate teams should evaluate the aspects of BIA relevant to their area

Main steps (3)

- Determination of preventive controls
  - Assessment of countermeasures and protective measures to reduce the risk and consequences of adverse events on data, business processes and personnel

- Organizing response teams
  - List of skills required to respond to IR, DR and BC and selection of necessary personnel

- Development of response strategies (contingency strategies)
  - Pr. backup and data recovery plans, organization of alternative locations, ...

- Development of subordinate plans
  - Activities for each area (IR, DR, BC)

- Plan testing, training and exercises
  - Checking the effectiveness of each of the subordinate plans

- Maintaining the plan
  - Periodic checking, evaluation of the plan and updating

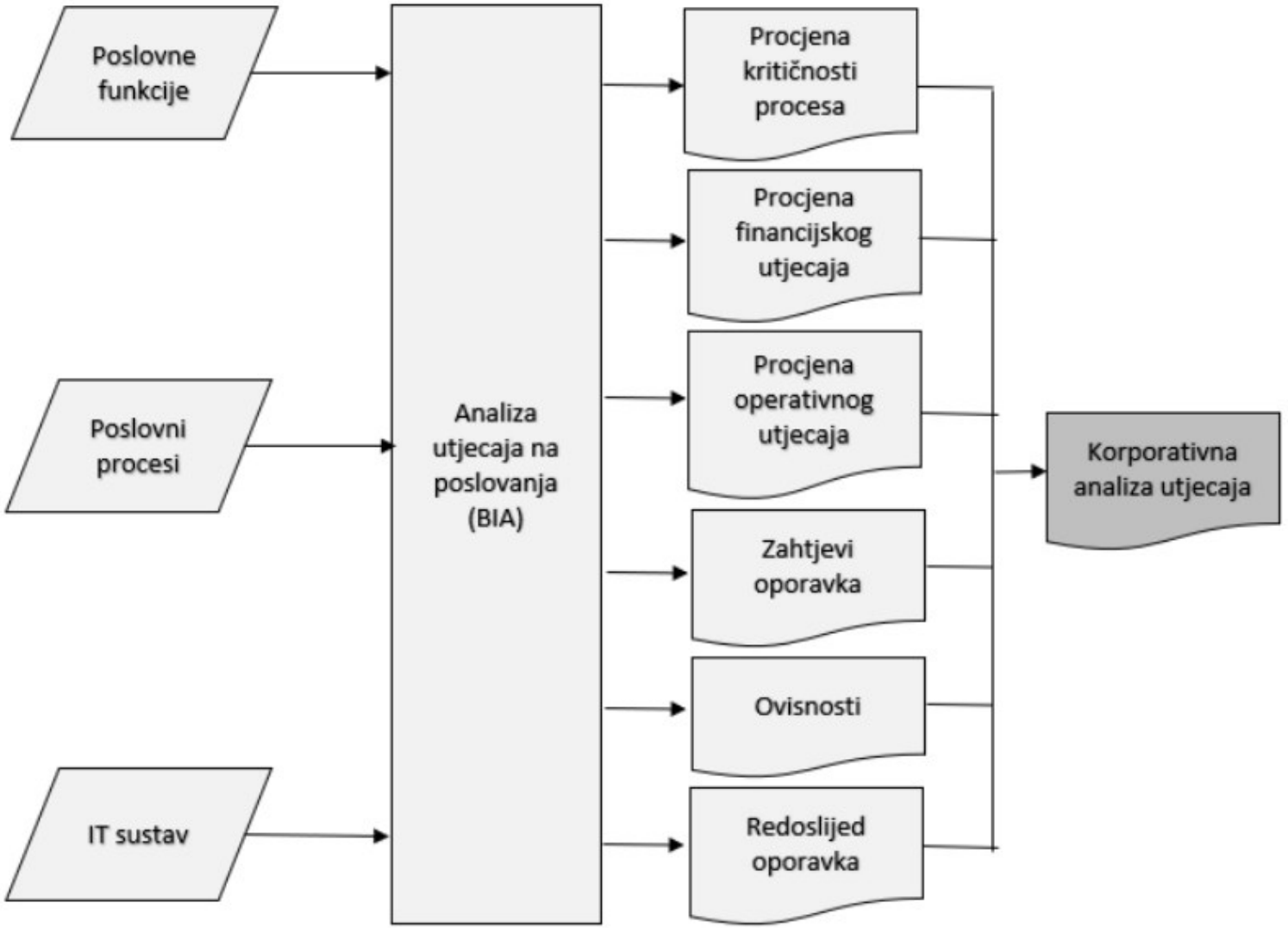
Analysis of the impact on business

- Business Impact Analysis (BIA)
  - Establishes organizational functions and their priorities, as well as information systems that support critical business processes
  - Risk management focuses on threats, vulnerabilities and attacks to determine controls to protect information
  - BIA assumes that controls can be bypassed, ineffective
- He tries to answer how it will affect
  - **Reach**: which organizational units and systems to cover
  - **Plan**: the data can be voluminous - consider the relevant ones
  - **Balance**: objective-subjective, emphasis on the knowledge and experience of the staff
  - **Goal**: determine key decision makers - information for making
  - **Tracking**: periodic verification that process owners and decision makers support the BIA process and outcome

BIA steps

- NIST SP 800-34 (National Institute of Standards and Technology)
  - Identification of key business processes and functions,
  - Determining the interdependence of information systems and business processes,
  - Determination of priorities and classification of business processes and functions,
  - Determining the impact of business process interruptions on overall business operations, with an emphasis on financial and operational impacts,
  - Determining required recovery times,
  - Determining prerequisites for business recovery,
  - Determining the order of recovery of individual processes and functions.

BIA result: corporate business impact analysis



Identification of business processes and functions and impact assessment

- **Critical functions**(critical functions) - necessary for the operation of org. (core)
  - IT perspective - an outage has serious/permanent security, operational and financial impacts
  - Acceptable recovery time is measured in hours

- **Essential functions**(essential functions) - very important, but not crucial
  - Pr. payment of wages to employees
  - Acceptable recovery time in the IT segment – a day or two

- **Required functions**(necessary functions)
  - Unavailability for an extended period can have a significant effect
  - Pr. E-mail or Internet access, business process support functions
  - Acceptable recovery time is measured in days

- **Preferred functions**(desirable functions) - small effect on business
  - Auxiliary functions that have developed over time to support business operations
  - Interruption can be an opportunity to revise them - it may turn out that they are not necessary
  - Acceptable recovery time - weeks or months

Recovery requirements

- Recovery target point - RPO (Recovery Point Objective)
  - Time tolerance of data loss, state of recovery by restoring a backup copy of data Time
  - between the last *backup* and interrupting event
    - Pr. weekly backup + outage on Saturday → RPO = 1 week

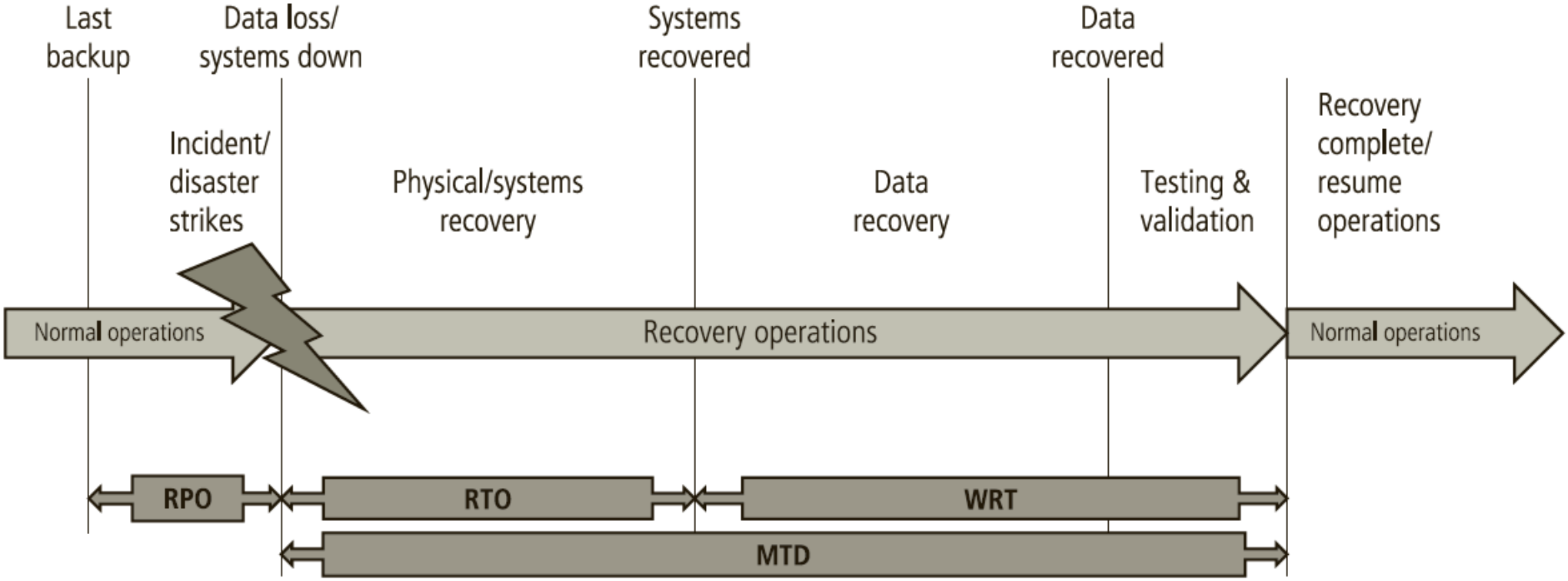
- Target recovery time - RTO (Recovery Time Objective)
  - Maximum recovery time resources that support the organization's mission
    - Computer systems, production devices, telecommunications, buildings and workspace
  - Time between interrupt event and system/resource recovery

- Work recovery time - WRT (Work Recovery Time)
  - Full recovery time business functions after resource recovery
  - Data recovery (electronic r*esters* and manual entry) + testing and validation

- Maximum acceptable downtime - MTD (Maximum Tolerable Downtime)
  - The maximum tolerable downtime/outage of the system measured by the duration of the unavailability of business processes
  - The period between the interrupting event and the start of normal operations

  - MTD = RTO + WRT

Analysis and prioritization of business processes



Interdependencies of business functions

- How and when will the interruption of a certain business function affect others?
- Is this function tied to any specific resources (certain suppliers, equipment)?
- Who are the key people to perform this function? What if these people are unavailable?
- How is this function performed - continuously, periodically, on a daily or weekly basis? Is there a critical time when it is necessary for business?
- What IT resources are necessary to perform this function?
- Are there any manual, workaround procedures by which it can be executed even if the information system is not available?

Impact Analysis Report

- Key processes and functions,
- Interdependencies of processes and IT resources,
- Criticality, i.e. the level of impact on business,
- Key roles and responsibilities of persons in charge of their implementation,
- Required recovery times,
- Financial, operational, legal, personal effects of unavailability,
- Manual procedures for business continuity in case of unavailability.

Incident response

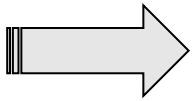
Incident Response Planning (IRP)

- Identification and classification of incidents and corresponding responses

- Incident response planning team (IR team)
  - Develops incident response plans

- Incident Response Team
  - Computer Security Incident Response Team (CSIRT)
  - Executes plans in response to an incident

- Phases of incident response
  - planning
  - detection
  - reaction
  - Recovery



Establishment of an incident response team

- Related terms

- Computer Security Incident Response Team (CSIRT)
  - service responsible for receiving, reviewing and responding to reports of computer security incidents - an organizational body, but it can also be external

- Information Security Incident Response Team
  - Information Security Incident Response Team (ISIRT)
  - according to ISO/IEC 27035:2011 (no longer valid)
  - a team of suitably skilled and reliable members of the organization who handle information security incidents throughout their life cycle

- Computer Emergency Response (CERT)
  - team for ICT incidents, organizational, more often national, where it can be called differently
  - Pr.https://www.cert.hr/ ,https://www.cert.hr/csirt_specifikacija/

Incident Response Policy

- NIST 800-61, Rev. 2, The Computer Security Incident Handling Guide
  - Statement on the purpose and objectives of the policy
  - Reach - to whom what applies and under what circumstances
  - Definition of incidents and related terms
  - Organizational structure, definition of roles, responsibilities and powers
    - Seizure or shutdown of equipment, surveillance of suspicious activities, reporting of perpetrators
    - Information sharing (what, who, when, how)
    - Escalation procedure
  - Prioritization or severity rating of incidents
  - Performance measurement (access control, security walls, DNS, ...)
  - Reporting and forms

Incident response planning

- The assumption is that there is a CSIRT
  - Competences, on-call,...
- Format and content
  - Organized instructions on handling procedures
  - ... during and after the incident
- Accommodation - IR plan protection
  - At hand, but so that the attacker does not discover them
  - Physical binders near admin stations, cabinets, encrypted files
- Testing
  - Checklists, structured walk-through, simulation, complete interruption

- 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.

Incident detection

- Indicators possible incidents
  - Unknown files
  - Unknown processes
  - Unusual consumption of computer resources
  - Unusual system crash

- Indicators likely incidents
  - Activities at unusual times (network traffic or "idle" file access)
  - Emergence of new credentials
  - Attacks reported by users
  - IDPS (Intrusion Detection / Prevention System) notifications

Incident detection (2)

- Indicatorscertain onesincidents
  - Using inactive credentials
  - Changes to log entries (relative to backup)
  - The presence of hacking tools
  - Notification of partner or partner (partner,*peers*)
  - A message from a hacker - a "gotcha" on a website or an email message from a "secure" account

- Other indicators
  - Loss of availability - unavailable system
  - Loss of integrity - corrupt files or data
  - Loss of confidentiality - notification of a data breach or disclosure of information that was thought to be protected
  - Violation of policy - events in violation of org. security policies
  - Violation of the law - the law was violated in which the org. resources

Reaction - key terms

- Alert message
  - Description of the incident with sufficient information
  - That each person knows which part of the IR plan to implement without slowing down the notification
- alert list (alert roster)
  - Contacts to be notified about the occurrence of the incident
  - Hierarchical roster
    - A list of warnings where the first person calls several others, and those on
    - faster but less precise
  - Sequential roster
    - An alert list where one person calls everyone on the list
    - more precisely but longer

Reaction - procedure

- Help desk, user or system administrator
  - They invite "real people" from the warning list
- Documenting the incident
  - Who, what, when, where, why and how
  - Case study, learning
  - Proof of correct behavior
  - A foundation for future simulations
- Strategies for suppressing incidents and regaining control
  - Filtering messages, blocking sockets, disabling credentials, reconfiguring sig. rocks, temporary stoppage of services and processes

Recovery from the incident

- Investing efforts according to priorities - following the plan

- Damage evaluation
  - Right now, for days, for weeks
  - System and data storage assessment
  - Log study, computer forensics, evidence collection

- Recovery
  - Vulnerability identification
  - Installation, replacement, upgrade protection
  - Recovery of data, services, processes
  - Continuous monitoring/surveillance of the system
  - Restoring trust

- After Action Review (AAR)

Disaster recovery

Disaster

- unwanted and unexpected harmful event that the organization
- prevents the performance of critical business functions
- through an indefinite period of time i
- results in great damage (not only financial) to her business

- Some examples
  - unavailability of the organization's main location due to a natural disaster or fire,
  - unavailability of the IT infrastructure at the main location due to a major hardware or software failure,
  - unavailability of key employees of the organization due to the epidemic,
  - long-term interruption of electricity supply,
  - disruption of key supplier services

Content of the disaster recovery plan (DR plan)

- List of IT assets
  - inventory of hardware, systems and applications
- Risk evaluation
  - for each key IS; probability, consequences
- Classification of importance
  - critical, others
- RPO and RTO
- List of activities - procedures for establishing business continuity
  - Short-term - basic functionalities
  - Long-term - business returns to normal

Recovery activities

- Hardware recovery
  - Replacement of components at the main or backup location
  - Servers, network equipment, firewall, IP/DS
- Recovery of operating systems
  - OS and main services (eg DNS, AD)
- Recovery of databases and archive records
- Data store recovery
  - *Storage*, backup hardware (Storage Area Network – SAN)
- Application recovery
  - Data, sync with backup location, check
- Testing recovery procedures

Disaster recovery levels (IBM, 2007)

- Level 0 – no data storage at backup location
  - The data is not stored in another location
  - Recovery is only possible using the system at the primary location

- Level 1 – Backing up data with a cold location
  - Data is stored on disks/tapes and physically sent to a backup location
    - Pickup Truck Access Method (PTAM)
  - Reserve cold site (cold site)
    - only basic infrastructure such as furniture, power supply, network cabinets and sockets
    - establishment of HW and SW, and restoration of backup copies of data
  - A cheap solution, the continuation of work is usually only possible after a few days

Disaster recovery tiers (BC tier 2 - 4)

- Level 2 - Backing up data with a hot location
  - Backup copies are physically sent to the backup location - PTAM
  - Backup hot location (host site)
    - on which an active backup system with appropriate HW and SW is installed, so data recovery
  - More expensive solution, continuation of work within 24 hours

- Level 3 – Electronic vaulting
  - BC2 + Critical data electronically to a backup location (remote backup service)
  - More efficient, continuation of work in ten hours

- Level 4 – Active Reserve Location
  - All data periodically electronically copied to a backup location (point-in-time copies)
    - *Batch/Online Database Shadowing and Journaling, Global Copy, FlashCopy, …*
  - Data loss up to several hours

Disaster recovery tiers (BC tier 5 - 7)

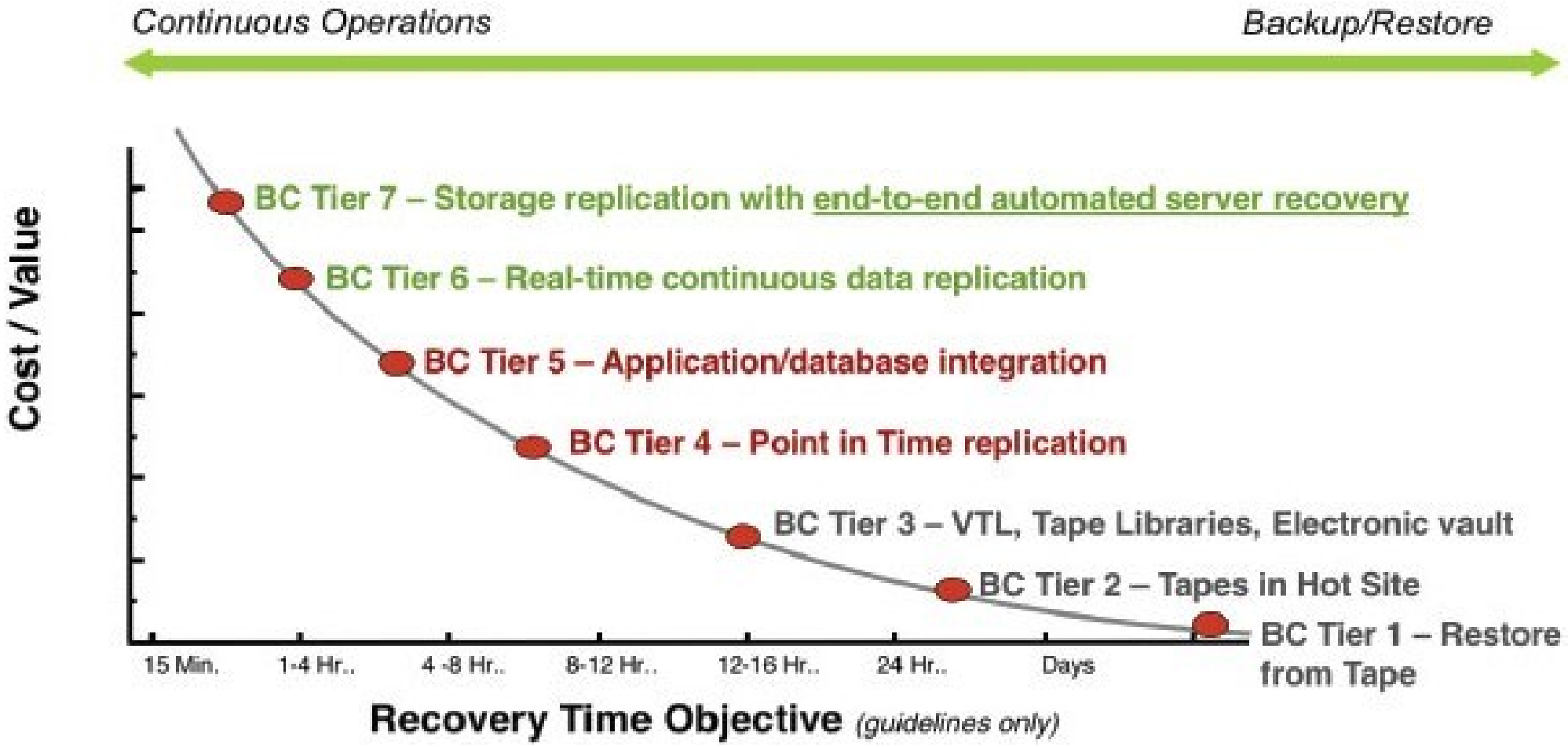
- Level 5 – Transaction Integrity
  - Application data and data from BP are copied at the transactional level to disks in the backup location (two-phase commit, remote replication, ...)
  - Recovery depends on the software used

- Level 6 – Minimal or no data loss
  - All data (regardless of the application) is "immediately" copied from the primary to the backup
  - Electronic (real-time storage mirroring, server mirroring), most often by disk-mirroring

- Level 7 – Fully automated solution
  - Level 6 upgrade where in the event of a disaster, IS automatically continues to operate on the hardware infrastructure, applications and data located in the backup location without any interruption or data loss

Recovery levels and business continuity

- BC1-3 *backup/restore*, BC4-5 rapid recovery, BC6-7 continuous availability



Backup location variants

- Cold – infrastructure, Warm – no applications, Hot – complete configuration

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

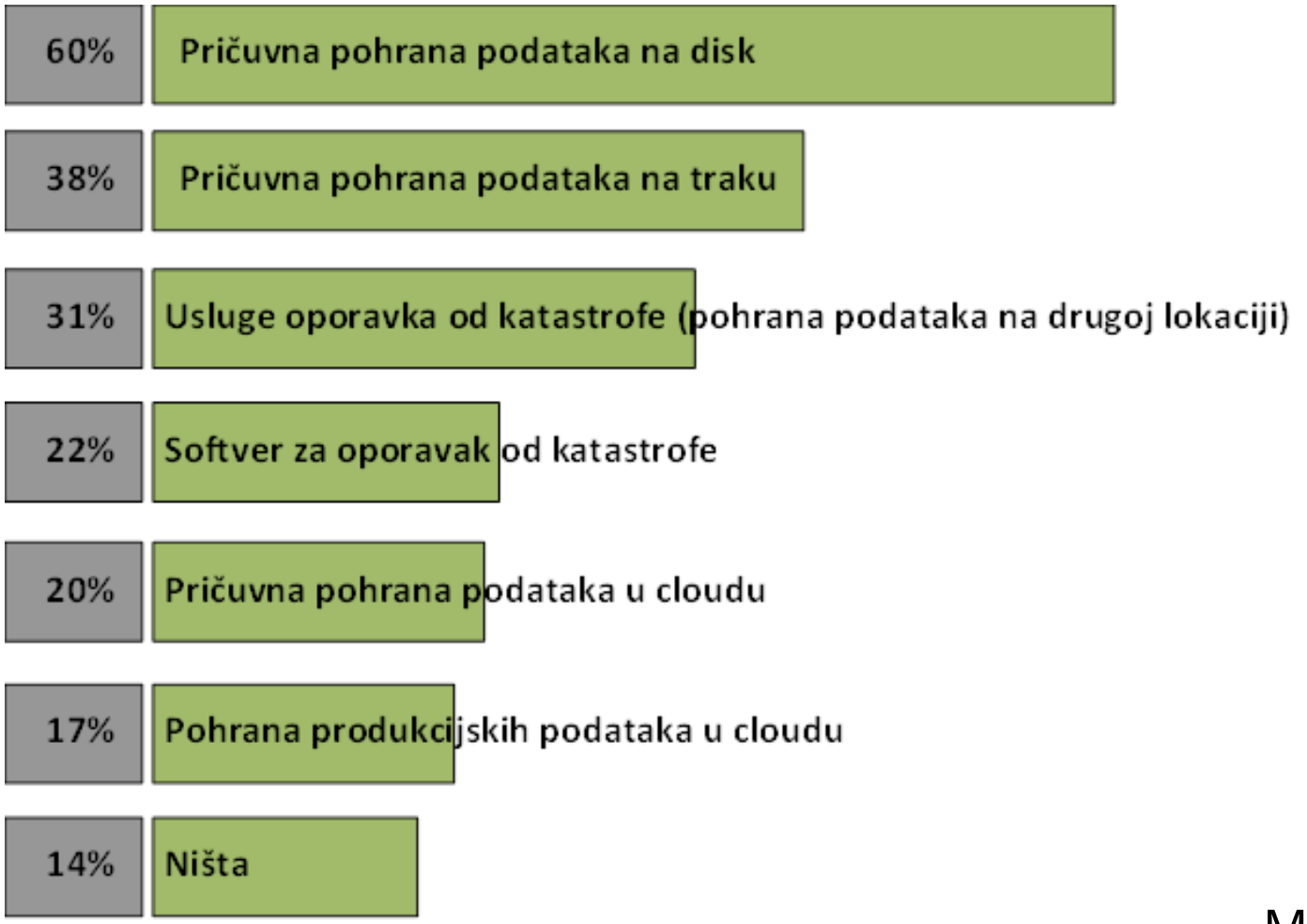
Procedures for switching from primary to backup location and vice versa

- ***Failover*(activation)**
  - Automatic continuation of work on the backup server, computer or network component in case of failure of the primary P/RK/MK
  - Real automated *failover* only possible at BC7 level

- ***Switchover*(roll switch)**
  - Controlled change of roles, usually manually at the planned time
  - Preparation for maintenance - installation of patches, upgrades, ...
  - Also to switch to backup when it is *failover* too complicated or too expensive

- ***Failback***
  - After training the system at the primary location
  - Restoring changes to data and applications
  - Ideally (BC7) automatically
  - In practice, with minor or major data loss, depending on the solution

Disaster recovery tools and technologies



- DRaaS - DR as a Service

Backup as a Service

aaS

m Cloud Connect

ation

staring Site Recovery

with

neither

wrestle

with

ation

re ESX, ESXi

- MS Hyper-V

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

Business continuity

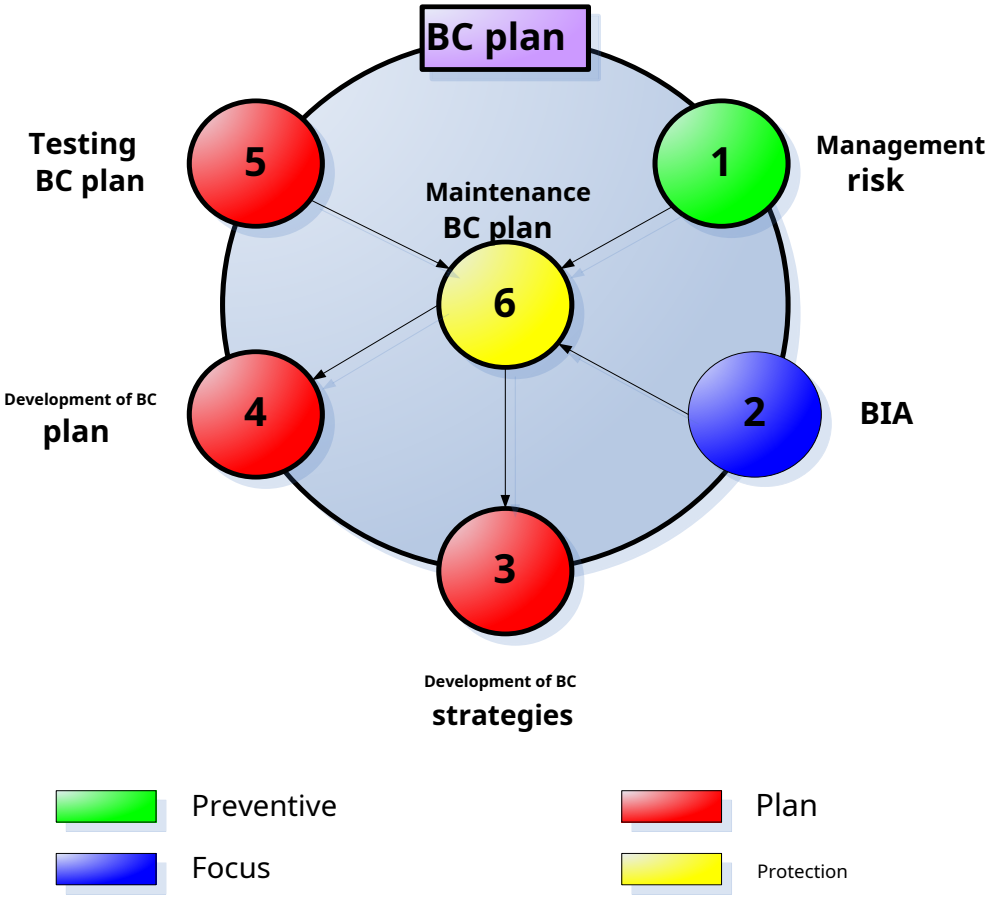
Business continuity planning

- An organization's efforts to continue critical functions in the event of a primary site outage
  - Senior management - development and implementation of BC policy, plan and teams

- Establishment of a business continuity management system (Business Continuity Management System - BCMS), according to the norm:
  - 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

Business continuity planning process

- The process follows four key principles: *Focus, Prevention, Plan, Protection*
  - which are implemented in the BC program through a six-step planning process:



Business continuity planning

- Risk management
  - Assessment of threats and risks for business continuity, risk control

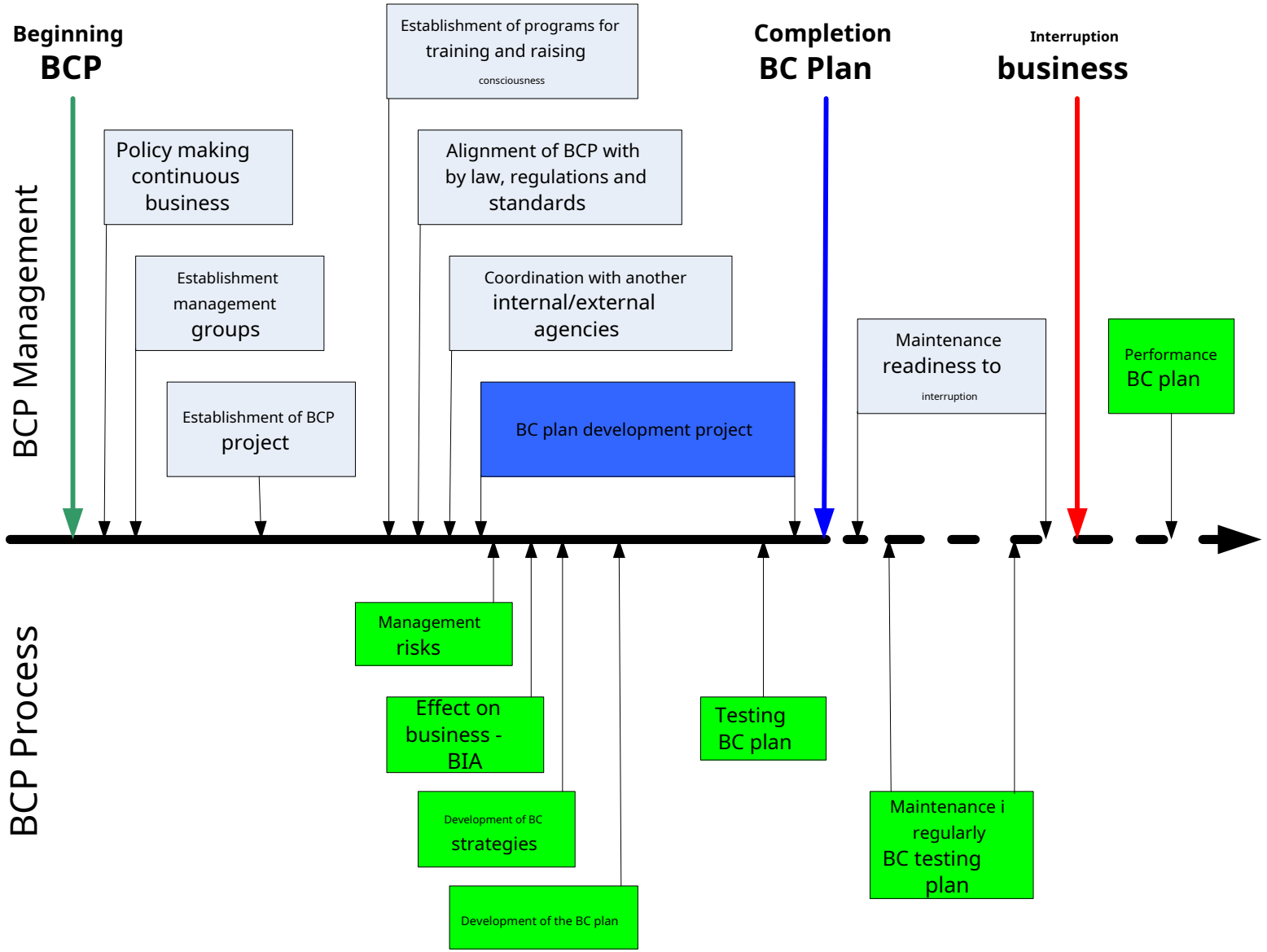
- Business Impact Analysis (BIA)
  - Identification of key business functions and processes, analysis of possible consequences
  - Identification of requirements for recovery after the occurrence of a disaster

- Development of a continuous business strategy
  - Evaluation of requests for recovery of interrupted key business processes.
  - Establishing solutions that meet requirements, choosing cost-effective solutions

- Development of the BC plan
  - Protection of key processes and assets from various threats and risks
  - Recovery of key business processes and resources in a safe and timely manner

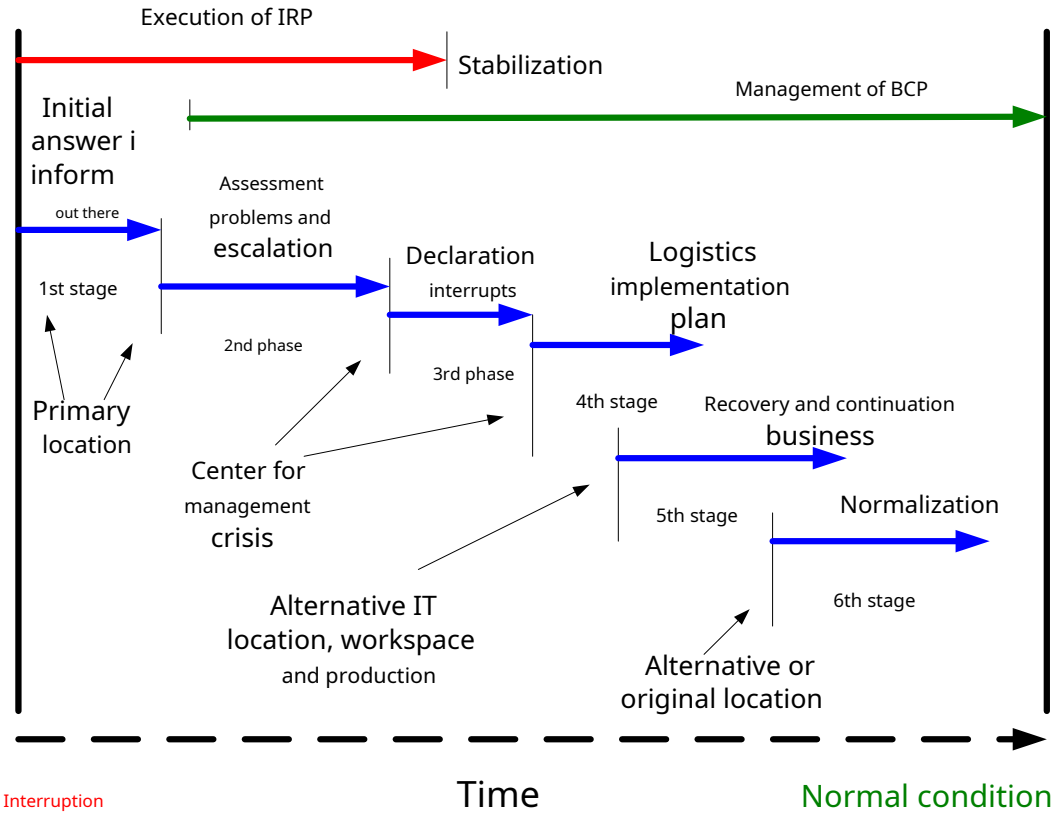
- BC plan testing
  - Testing the ability and effectiveness of the recovery team Testing the
  - ability and effectiveness of suppliers of goods and services

- Maintenance of BC plan


Beginning
BCP
Establishment of programs for training and raising consciousness
Completion
BC Plan
Interruption
business
BCP Management
Policy making continuous business
Alignment of BCP with by law, regulations and standards
Establishment management groups
Coordination with another internal/external agencies
Establishment of BCP project
BC plan development project
Maintenance readiness to interruption
Performance BC plan
BCP Process
Management risks
Effect on business - BIA
Development of BC strategies
Development of the BC plan
Testing BC plan
Maintenance i regularly BC testing plan

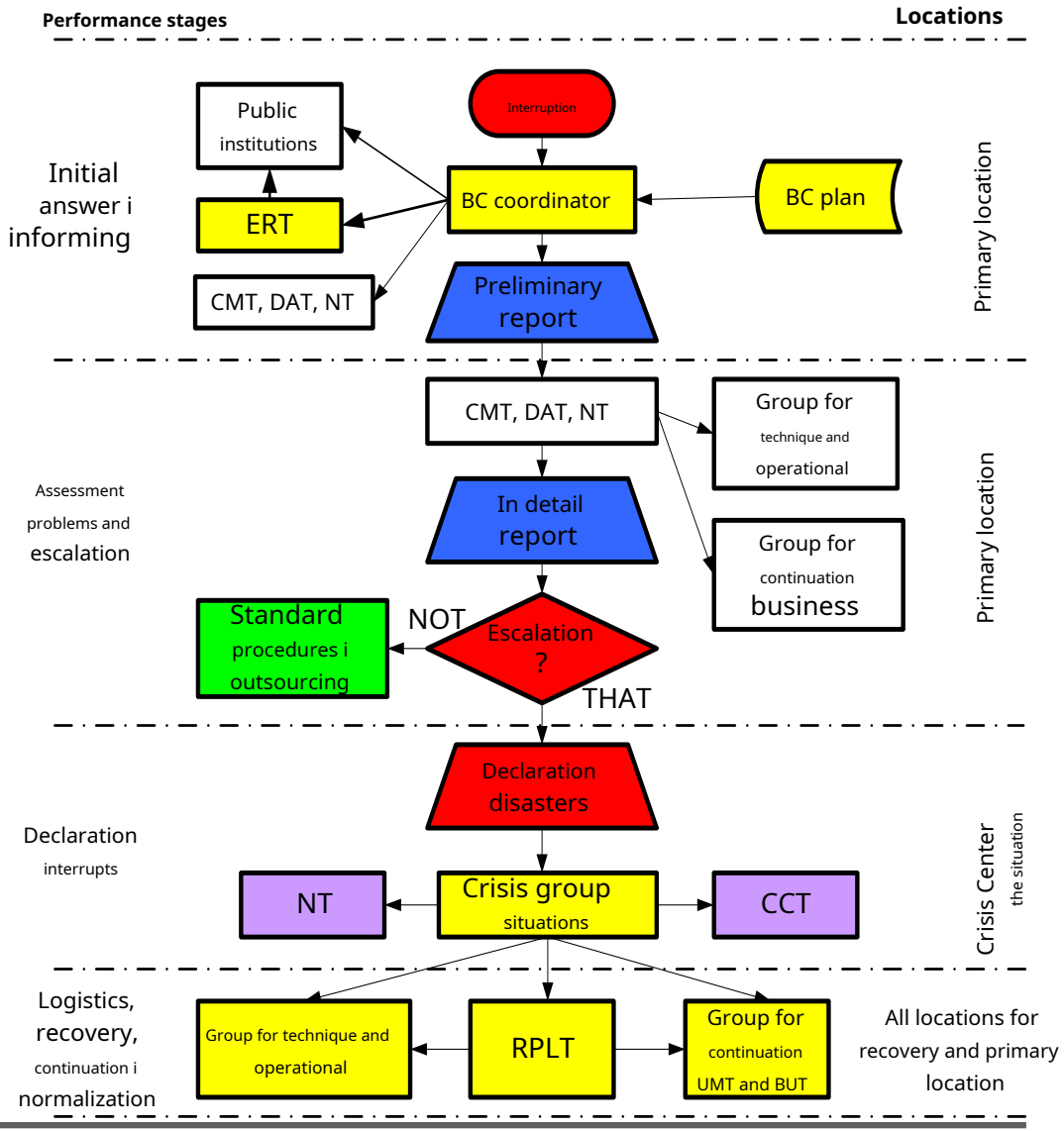
Execution of plan BC

- Initial response and notification
  - preliminary problem report
- Problem assessment and escalation
  - detailed problem report
- Statement on disaster / disruptive event
  - declaration of a disaster / disruptive event
- Implementation of the logistics plan
  - mobilization of teams, backup media, critical resources and devices
- Recovery and continuation of business
  - recovery of critical IT and non-IT resources and continuation of the process
- Normalization
  - operational status as it was before the interruption occurred



Roles and responsibilities in the implementation of the BC plan

- 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



References

- 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