Temple university

Auditing a business continuity management – BCM

November, 2015

Auditing BCM
Agenda

1. Introduction
2. Definitions
3. Standards
4. BCM key elements

Is better to be prepared to a disaster that could never happened, instead, something wrong happens and we are not prepared for it

Introduction

The need for Continuity Planning

Disasters can strike quickly and without warning,

- Floods, earthquakes, tornadoes, hurricanes, terrorist attacks, …

Business are vulnerable to the impact of not only major calamities but also minor business disruptions,

- Power outages
- IT system failures: v.g. malware or just hacking, Communication failures
- Manufacturing equipment failures
- Hazardous material contamination
- Robbery or other criminal activity

Why are business continuity plans important?

They provide an organized, coordinated and consolidated approach to managing response and recovery activities following any unplanned incident or business interruption, avoiding confusion and reducing exposure to error;

They provide prompt and appropriate response to unplanned incidents, thereby reducing the impacts resulting from short and long-term business interruptions;

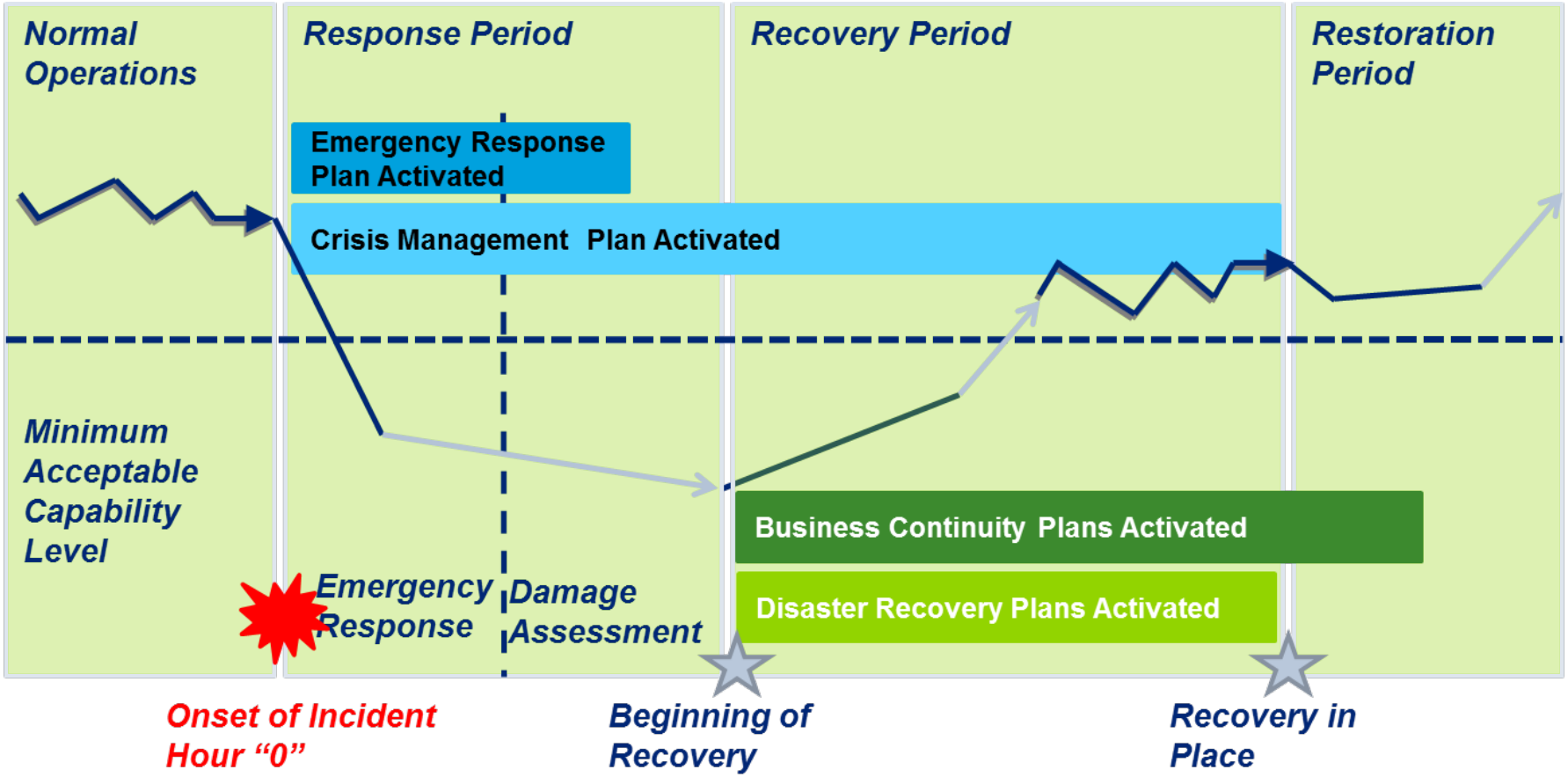
They recover essential business operations in a timely manner, increasing the ability of the company to recover from an unplanned incident.

Overall business continuity management

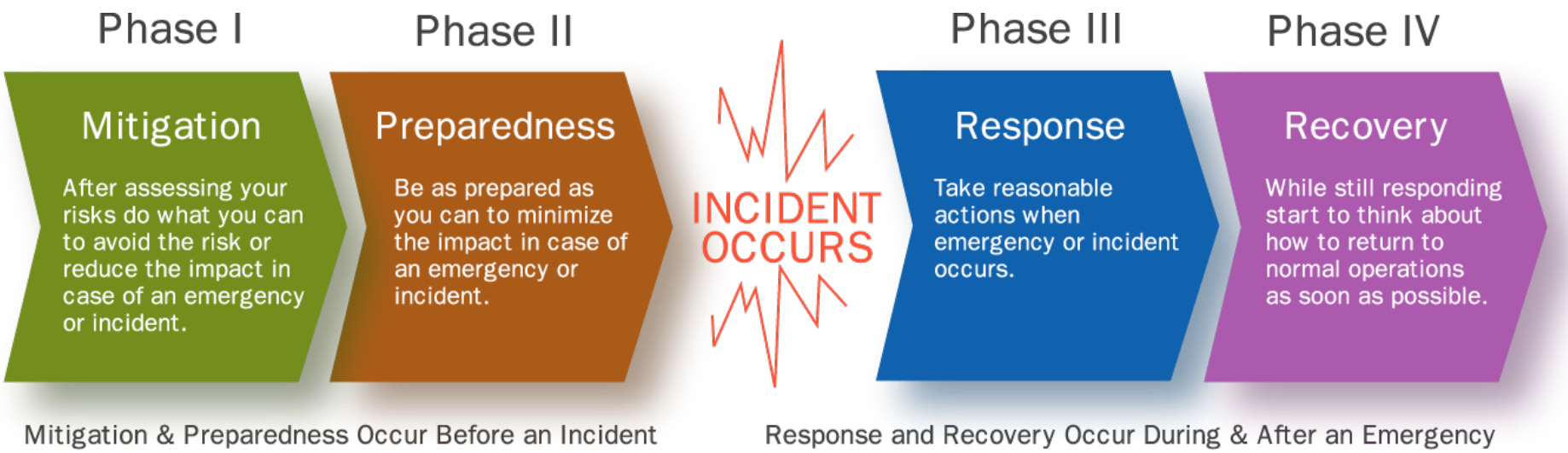
- Focuses on immediate response and life and safety
- Focuses on strategies and coordination of response
- Focuses on response to outbreak of infectious disease
- Documents recovery procedures for critical business functions
- Documents procedures for recovery of IT

Overall business continuity management

The general recovery process is illustrated in the next recovery timeline:



Overall business continuity phases



Definitions

Definitions
Disaster

Is an event, often unexpected, that seriously disrupts your usual operations or processes and can have long term impact on your normal way of life or that of your organization.

- He lost a laptop with the only copy of his thesis
- She lost her research and papers in the lab fire
- Payroll system failed the day before payday
- The death of a employee
- The recent tsunami
- An earthquake

Definitions
Resilience

Is the ability and capacity to withstand and adapt to new risk environments. A resilient organizations effectively aligns is strategy, operations, business systems, governance structure, and decision-support capabilities so that it can uncover and adjust to continually changing risks, endure disruptions to its primary earning, drivers and create advantages over less adaptive competitors.

Business resilience does not reduce the likelihood that an event will occur, but it does increase the likelihood that your company will withstand the event.

Definitions

Business Continuity Management - BCM

The goal of BCM is to provide the organization with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organization. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.

According to ISO 22301, a business continuity management system emphasizes the importance of:

- Understanding continuity and preparedness needs, as well as the necessity for establishing business continuity management policy and objectives.
- Implementing and operating controls and measures for managing an organization's overall continuity risks.
- Monitoring and reviewing the performance and effectiveness of the business continuity management system.
- Continual improvement based on objective measurements.

Definitions

Business continuity Planning

Is a **discipline** that prepares an organization to maintain continuity of business during a disaster through an implementation of a business continuity plan.

A business continuity plan is a **live** document that contains procedures and guidelines to help recover and restore disrupted processes and resources to normal operation status within an acceptable time frame.

It is:

- a process to minimize the impact of a major disruption to normal operations
- a process to enable restoration of critical assets
- a process to restore normalcy to MIT as soon as possible after a crisis.

It is not just: recovery of information technology resources

It is the phase of crisis management that follows the immediate actions taken to protect life and property and contain the event. It begins when the situation has been stabilized.

Definitions
According with ISO 22301:2012

BCM: Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realize, might cause, and which provides a framework for building organizational resilience with capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities .

BCP: documented procedures that guides organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.

BIA: process of analyzing activities and the effect that a business disruption might have upon them .

Standards

BCP standards

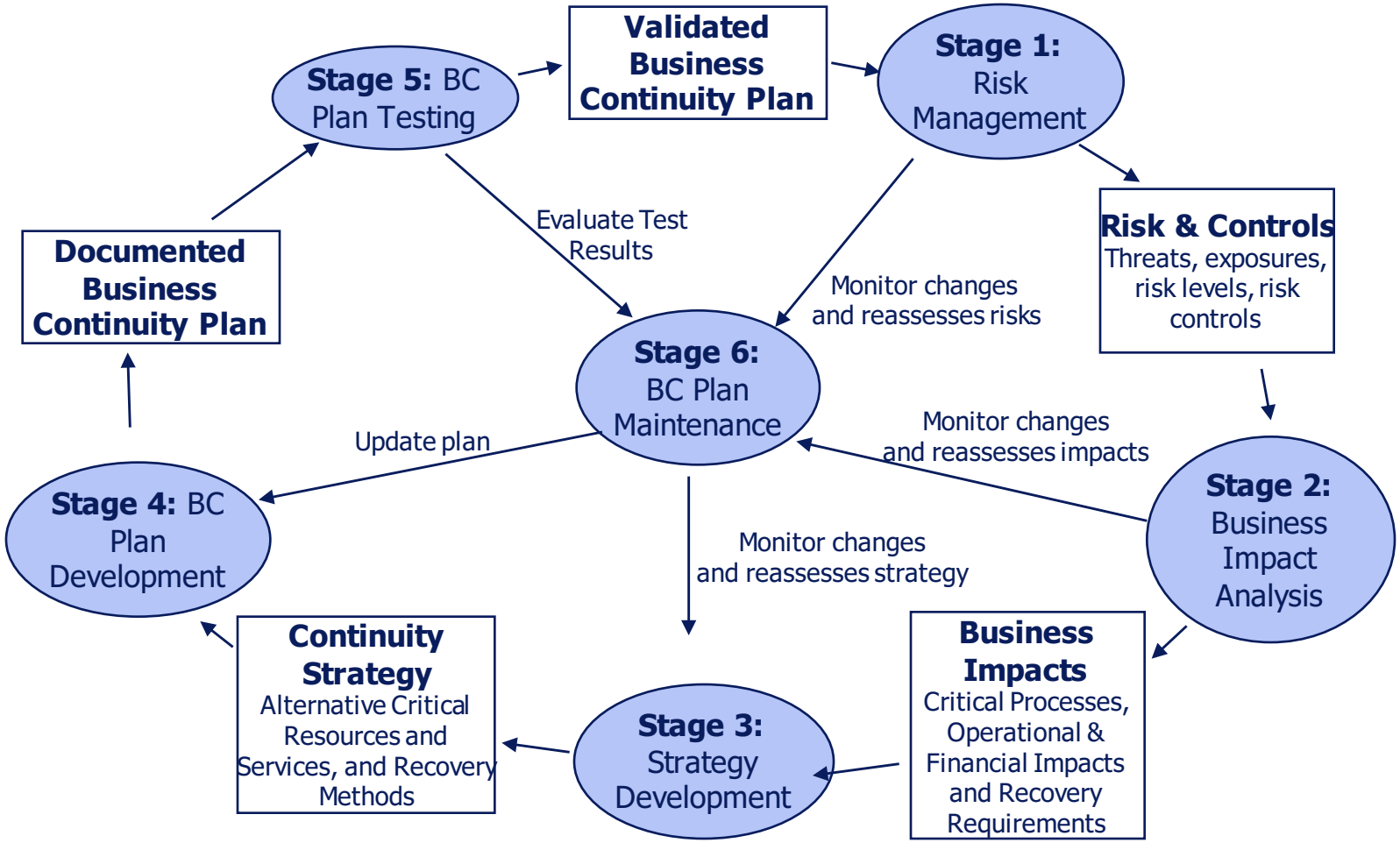
- BS25999 – British Standard
- NFPA1600: (National Fire Protection Association):Development, implementation, assessment, and maintenance of programs for prevention, mitigation, preparedness, response, continuity, and recovery.
- ASIS2009: Organizational resilience: security, preparedness, and continuity management systems – requirements with guidance for use
- FSA (Financial Services Authority) – Business continuity management practice guide.
- FFIEC (Federal Financial Institutions Examination Council) – business continuity planning process.

BCP standards

- ISO 24762 (5.11, 5.12, 7.1): provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management.
- ITIL Service continuity management.
- ISO 22301: specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
- ISO 27001:2013 (A14): Information security management.

Key elements

BCP Process


Stage 5: BC Plan Testing
Validated Business Continuity Plan
Stage 1: Risk Management
Risk & Controls
Threats, exposures, risk levels, risk controls
Evaluate Test Results
Monitor changes and reassesses risks
Documented Business Continuity Plan
Stage 6: BC Plan Maintenance
Update plan
Monitor changes and reassesses impacts
Stage 4: BC Plan Development
Stage 2: Business Impact Analysis
Monitor changes and reassesses strategy
Continuity Strategy
Alternative Critical Resources and Services, and Recovery Methods
Stage 3: Strategy Development
Business Impacts
Critical Processes, Operational & Financial Impacts and Recovery Requirements

BCP Process

Stage 1: Risk Management

Assesses the threats of disaster, existing vulnerabilities, potential disaster impacts and identifies and implements controls needed to prevent or reduce the risk of disaster

Stage 2: Business Impact Analysis (BIA)

Identifies mission-critical processes and analyzes impacts to business if these processes are interrupted as a result of a disaster

Stage 3: Business Continuity Strategy Development

Assesses the requirements and identifies the options for recovery of critical processes and resources in the event they are disrupted by a disaster

BCP Process

Stage 4: Business Continuity Plan Development

Develops a plan for maintaining business continuity based on the results of previous stages (stages 1 to 3)

Stage 5: Business Continuity Plan Testing

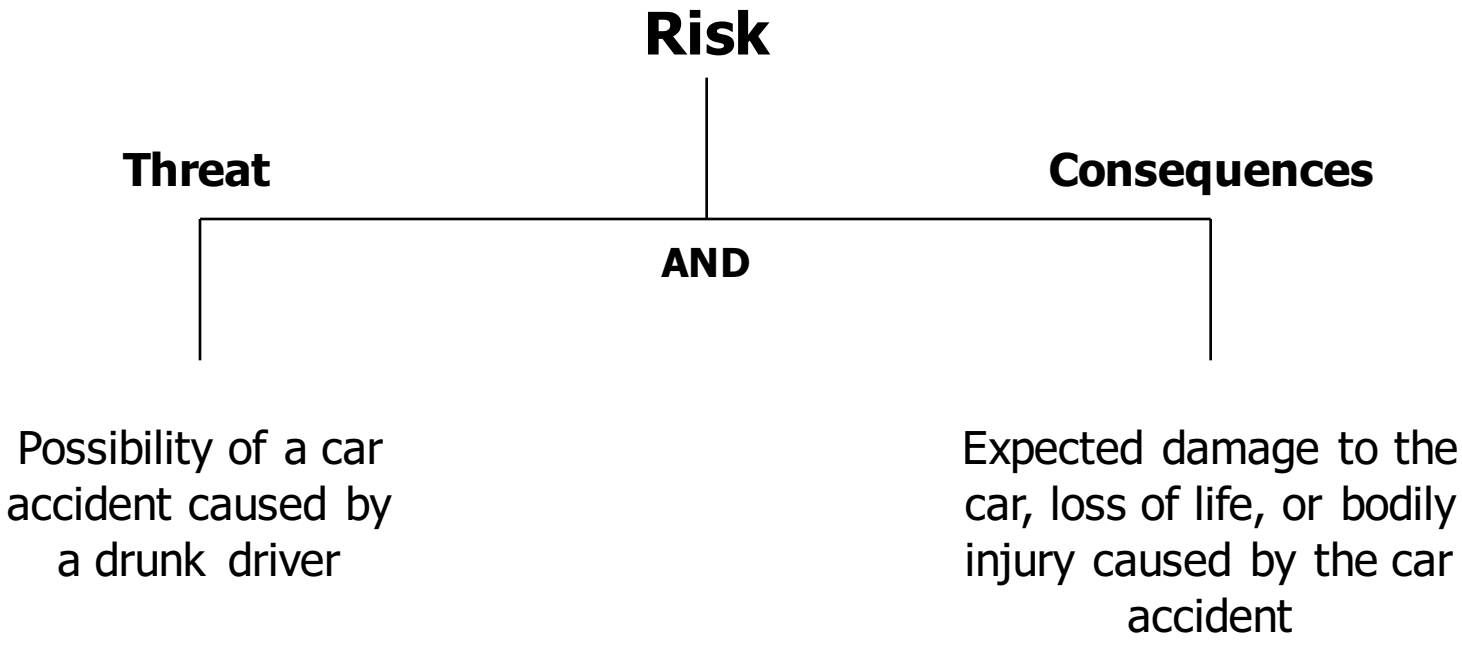
Tests the BCP document to ensure its currency, viability and completeness

Stage 6: Business Continuity Plan Maintenance

Maintains the BCP in a constant ready-state for execution

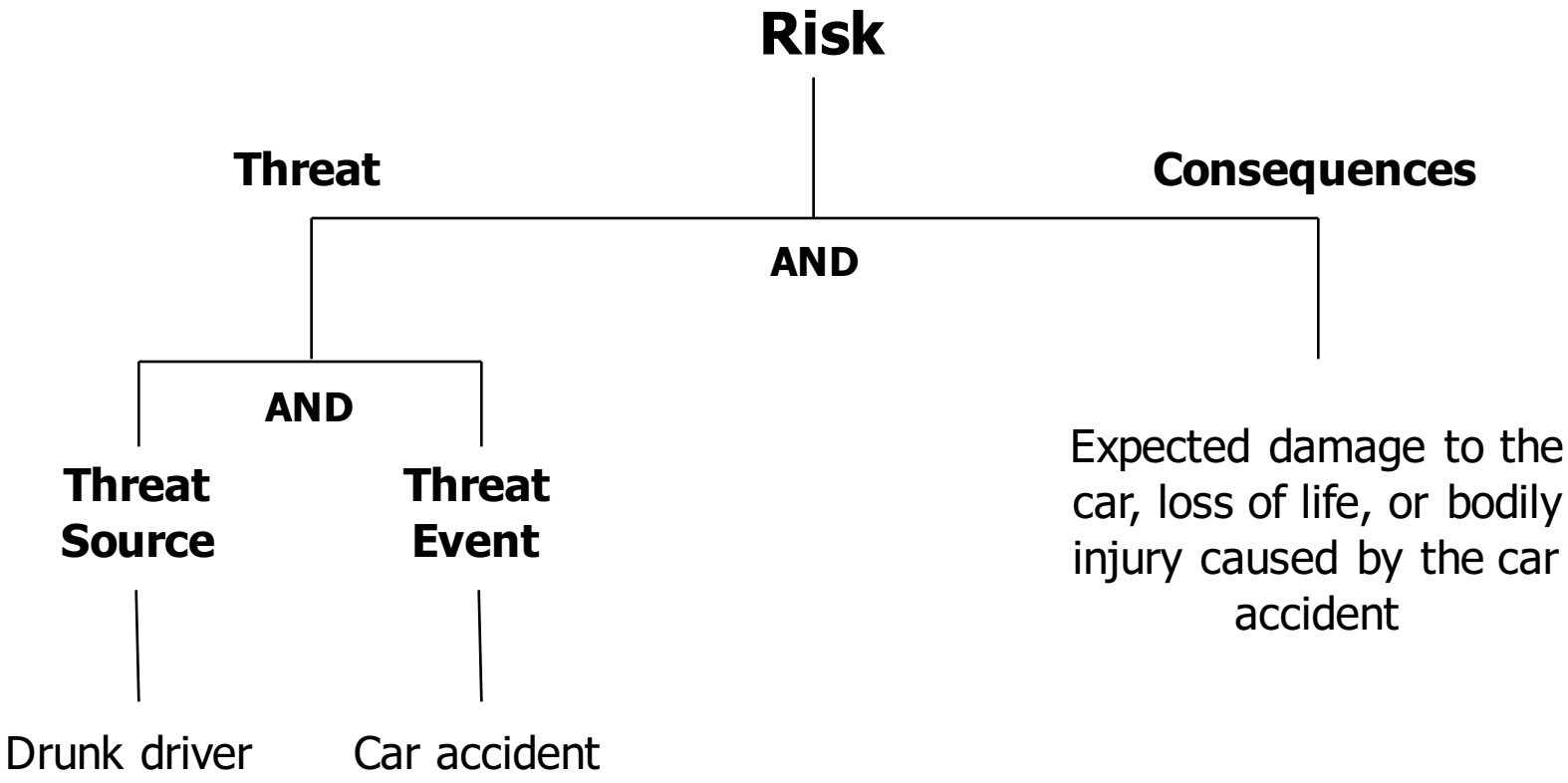
Stage 1: Risk Management

Graphical representation of a risk



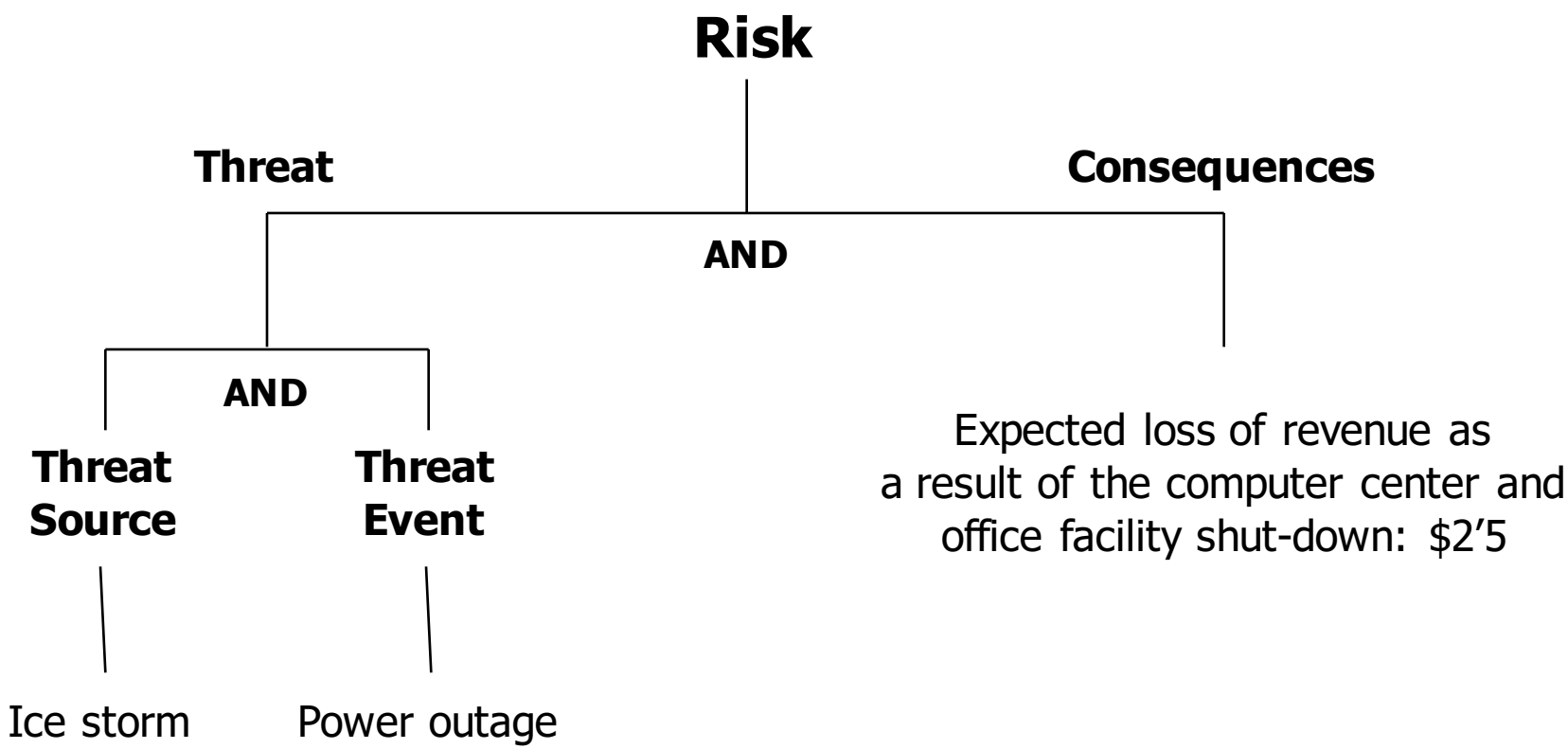
Stage 1: Risk Management

Decomposition of the threat components



Stage 1: Risk Management

Representation of an example business risk



Stage 1: Risk Management
Risk determination

Quantitative Metrics

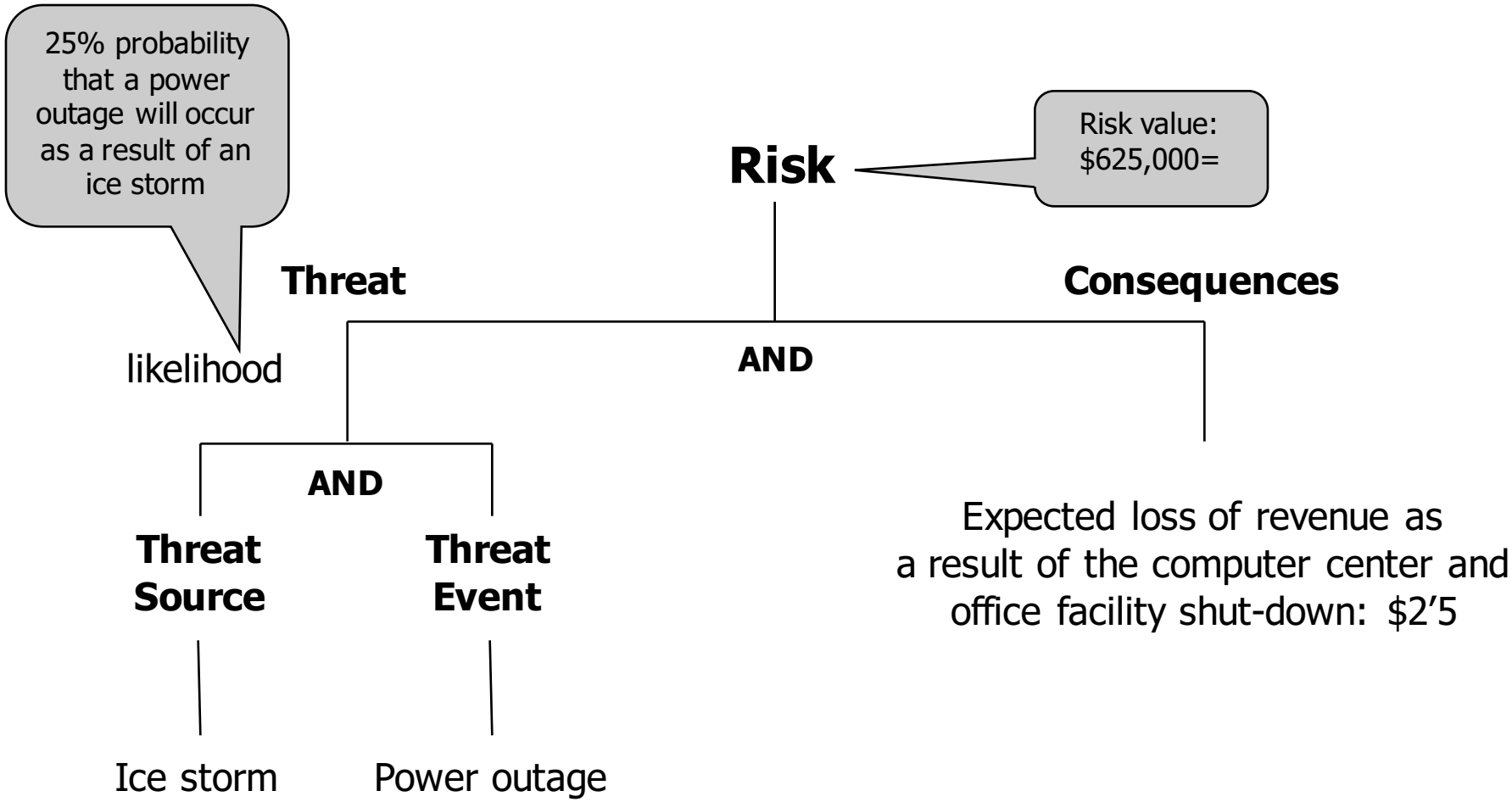
- Derived algorithmically using probability
- Considerable time and effort are required to gather and analyze data and to explain the results
- Usually you will need historical information

Qualitative Metrics

- Simpler computations (high, medium, low)
- Require less time
- But risk values are subjective and non-repeatable (they are based on judgments)

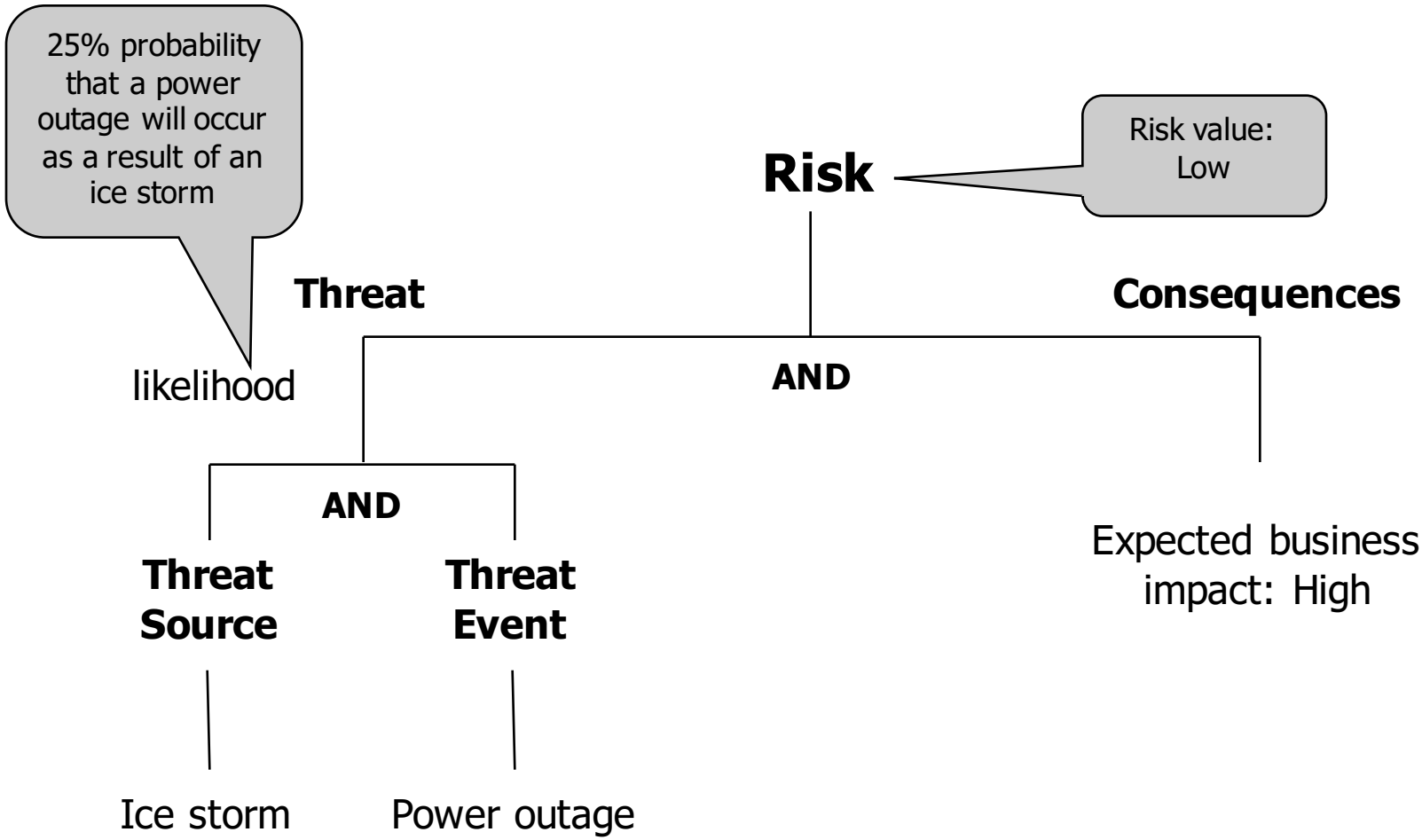
Stage 1: Risk Management

A risk with quantitative metrics



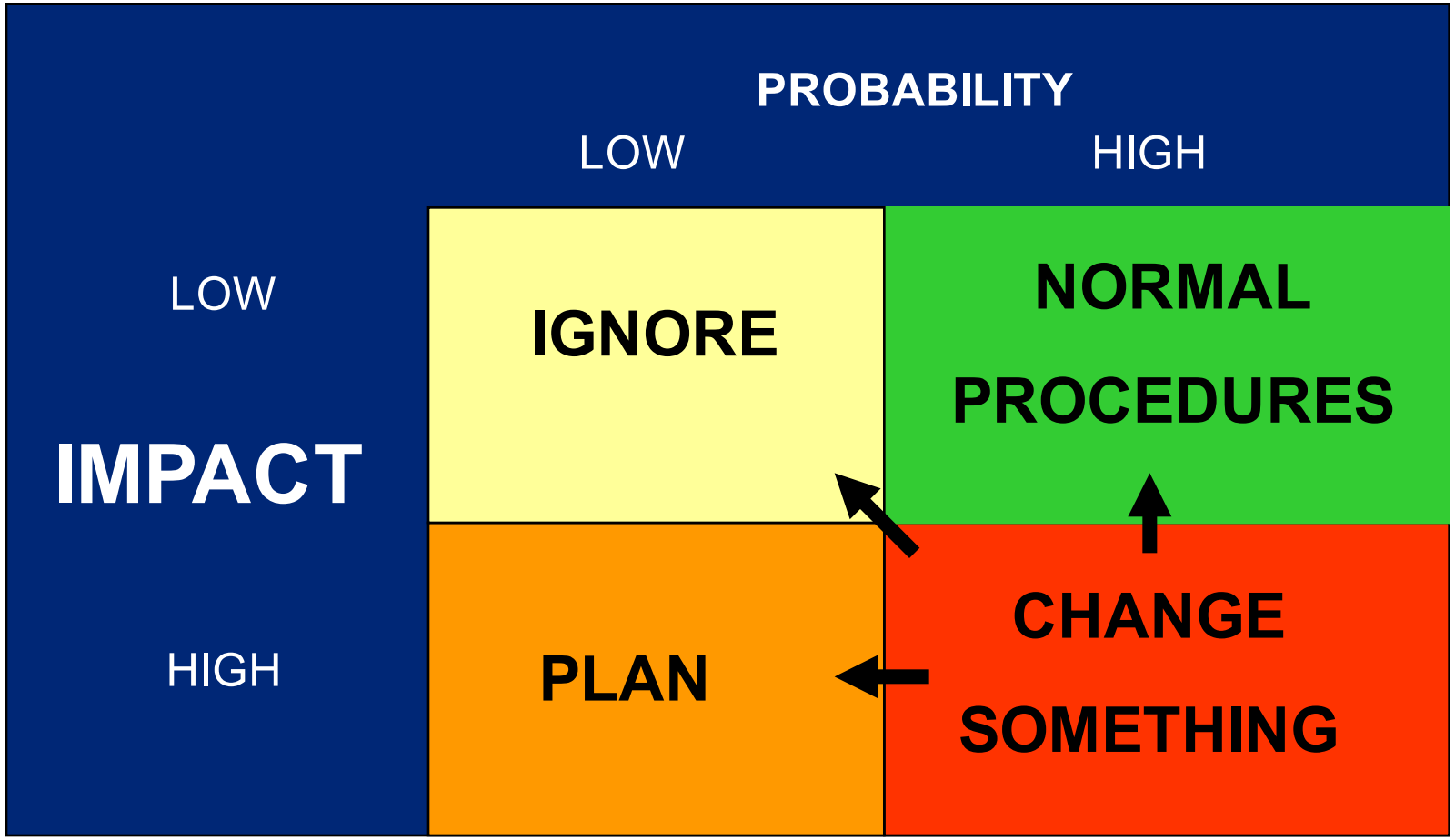
Stage 1: Risk Management

A risk with qualitative metrics



Stage 1: Risk Management

Matrix



Stage 1: Risk Management
Audit issues

- Scope (processes, facilities, buildings, equipment, technology, human resources, third parties)
- Risk universe used
- Qualification scales (quantitative -- qualitative)
- People interviewed (validation)
- Proper identification and test of controls (D&O – design & implementation, OE – operational efficiency)
- Proper documentation

Stage 2: Business Impact Analysis
Goals

It analyzes the financial and operational impact of disruptive events,

- Financial impact: monetary losses as lost sales, lost funding and contractual penalties
- Operational impact: non-monetary losses as loss of competitive edge, damage to investor confidence, poor customer service, low staff morale, and damage to business reputation

The BIA identifies the following information

- Mission-critical areas of the business and their processes
- Extent of potential operational and financial impact to the organization
- Requirements for recovering disrupted critical business processes

The BIA is a crucial link between the risk management stage and the business continuity plan stage:

- It identifies mission-critical areas and its <u>continuity requirements</u>

Stage 2: Business Impact Analysis

BIA approach

The BIA approach consisted of the four steps outlined below:

Identify Business Functions → **Collect and Validate Data** → **Analyze Data** → **Develop BIA Report**

- Defined Client function targeted in scope of BIA
- Obtained existing documentation including previously established BCPs, BIAs, process flow diagrams.

- Conducted BIA kickoff, BIA sessions and , Follow Ups
- Collected BIA data for scope business processes
- Requested & received validation/approval of all data captured

- Analyzed business process MTPD's
- Analyzed & aggregated quantitative and qualitative impacts
- Analyzed internal and external (Third dependencies)
- Identified minimum RTOs and RPOs for business applications
- Identified personnel, equipment/supplies requirements

- Developed a formal BIA report
- Summarized the BIA data
- Consolidated raw BIA data tables

Stage 2: Business Impact Analysis
Recovery Time Requirements

MTD (Maximum Tolerable Period of Disruption)

- Maximum downtime the organization can tolerate for a business process

RTO (Recovery Time Objective)

- Indicates the time available to recover disrupted systems/resources

RPO (Recovery Point Objective)

- It refers to the extent of data loss measured in terms of a time period that can be tolerated by a business process

WRT (Work Recovery Time)

- it's the time available to recover the lost data, work backlog and manually captured data once the system / resources are recovered or repaired

Stage 2: Business Impact Analysis

Business Terms versus IT Terms

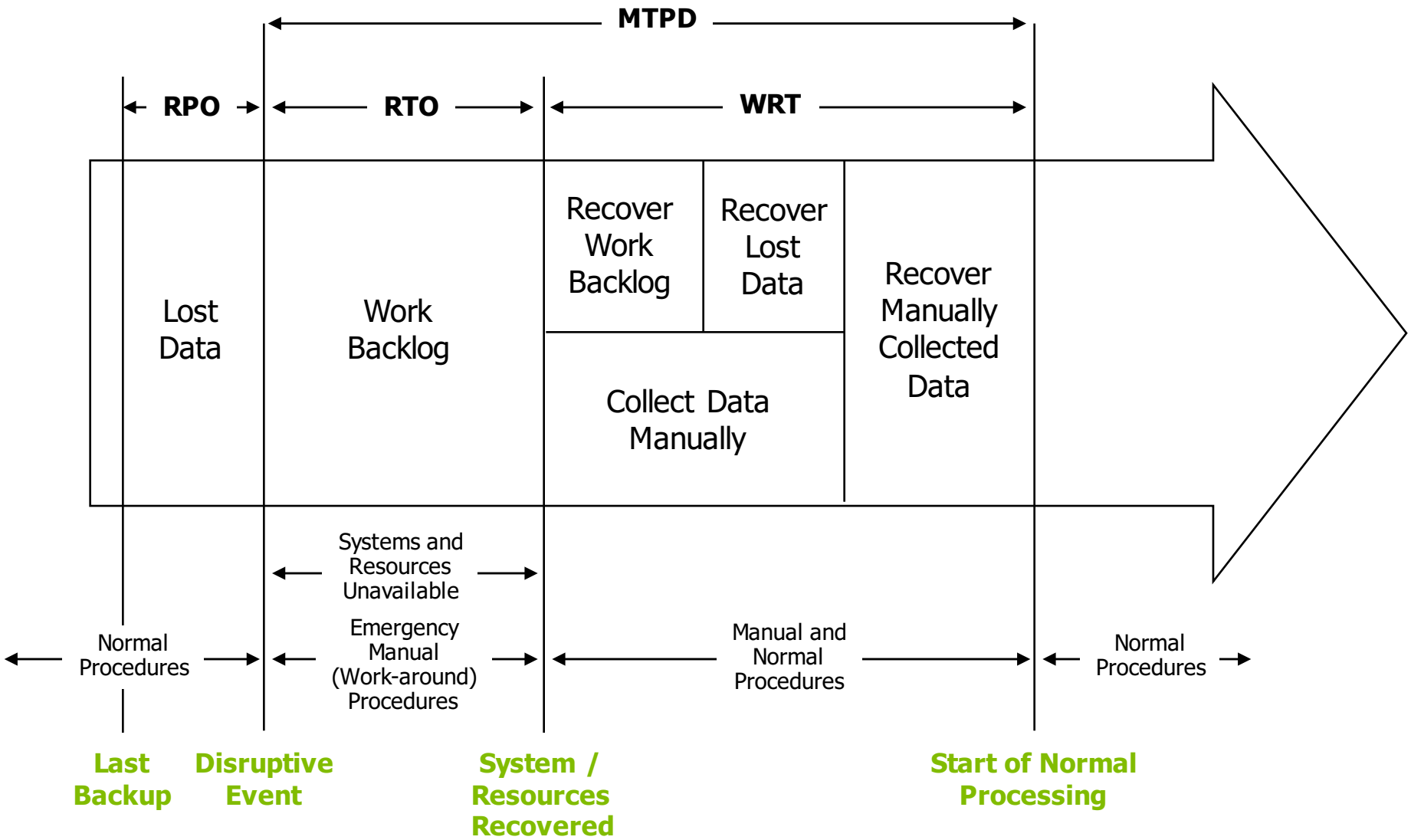
- Terms that start with “M” represent business facing timing parameters
- Terms that start with “R” represent IT facing timing parameters

Key terms for any organization

- Maximum Tolerable Period of Disruption (MTPD)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)

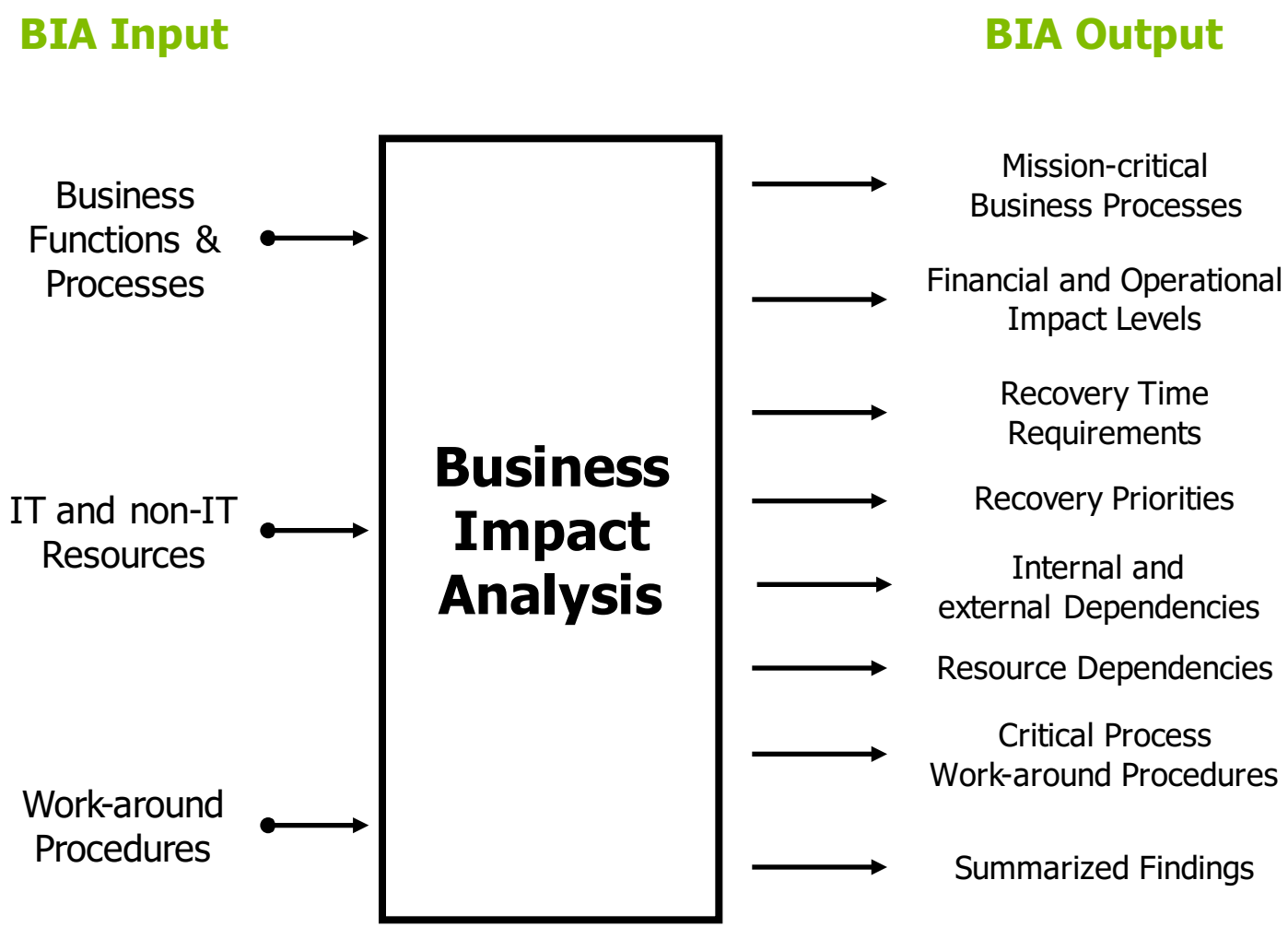
Stage 2: Business Impact Analysis

Disaster-recovery time frame



Stage 2: Business Impact Analysis

BIA input and output information



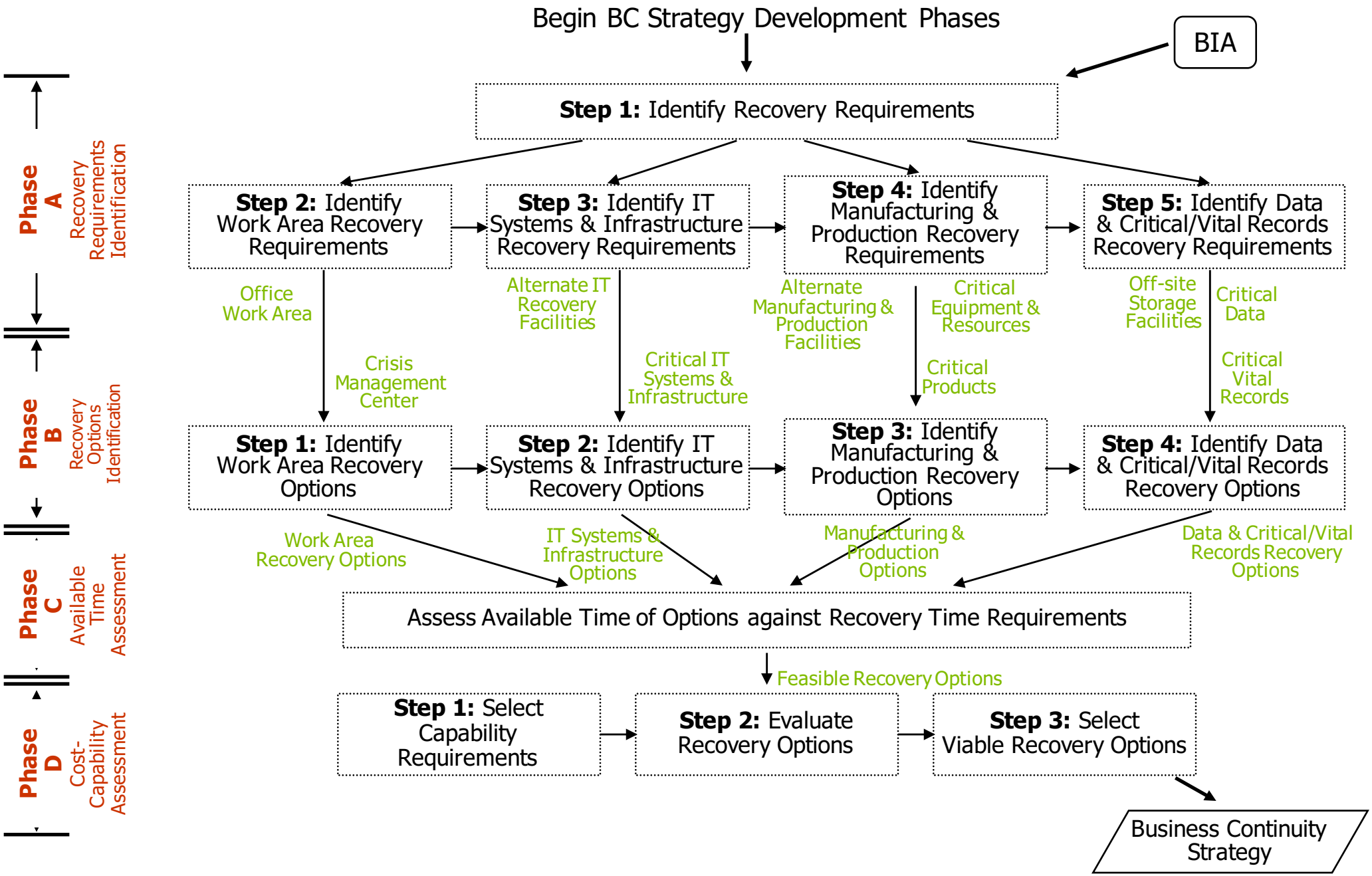
Stage 2: Business Impact Analysis
Audit issues

- Scope (processes, facilities, buildings, equipment, technology, human resources, third parties)
- Qualification scales (quantitative -- qualitative)
- People interviewed (validation)
- Identification of key processes / requirements
- Are the mission-critical business processes according with the business needs / requirements? What is the rationale of it? The process followed to obtain it, is well done?
- Are the RTO, RPO and MTPD right according with the business needs / requirements? The process followed to obtain it, is well done?
- Are logical the estimation of the financial and operational impact levels? Are these estimates according with the business needs / requirements? The process followed to obtain it, is well done?

Stage 2: Business Impact Analysis
Audit issues

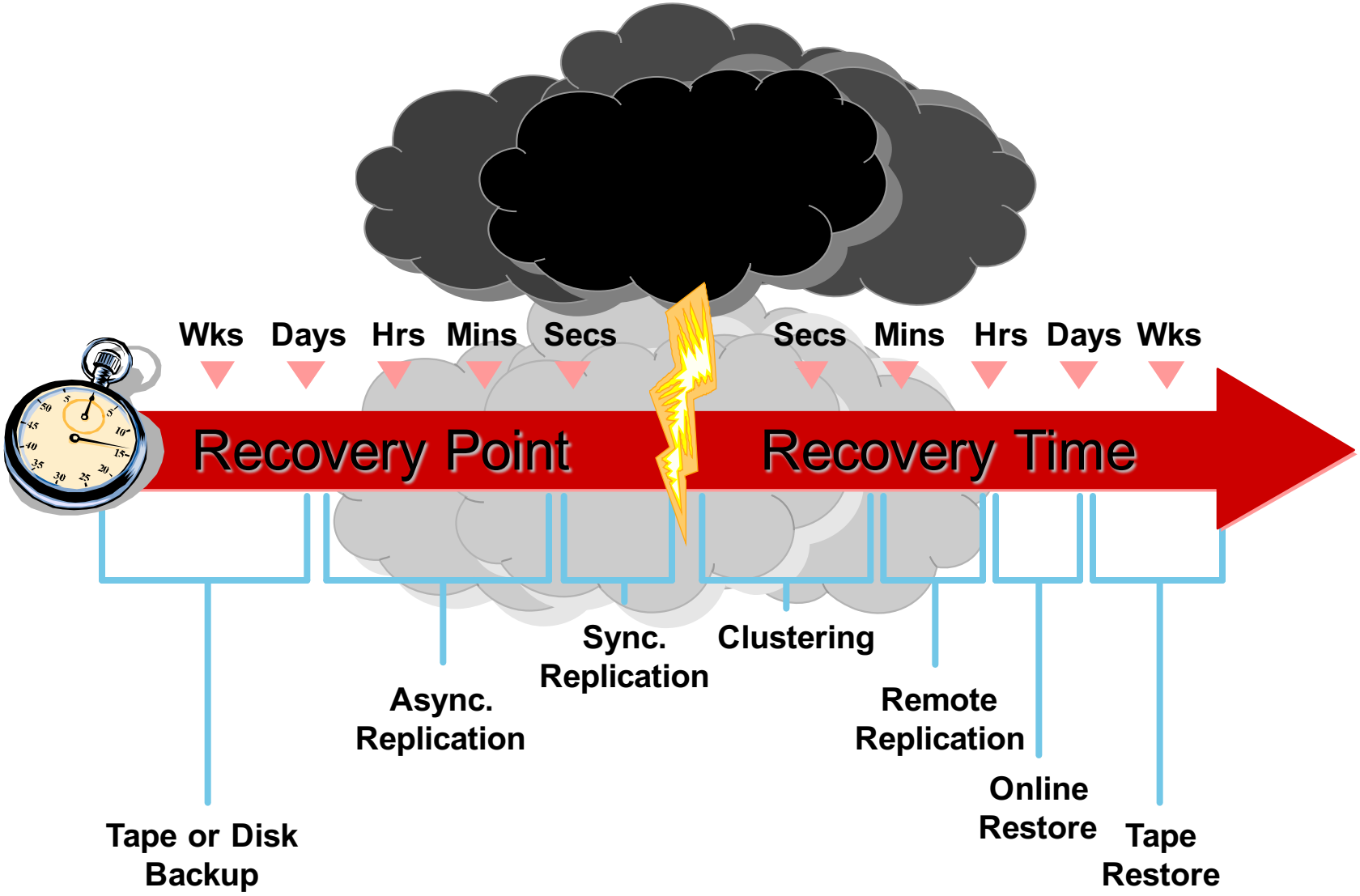
- The recovery priorities are based on the needs and requirements of the enterprise?
- Has been identified the main resources for each critical processes?
- Has been identified all the main internal and external dependencies?
- Has been identified and documented all the critical process work-around procedures?
- Proper documentation

Stage 3: strategy development



Stage 3: strategy development

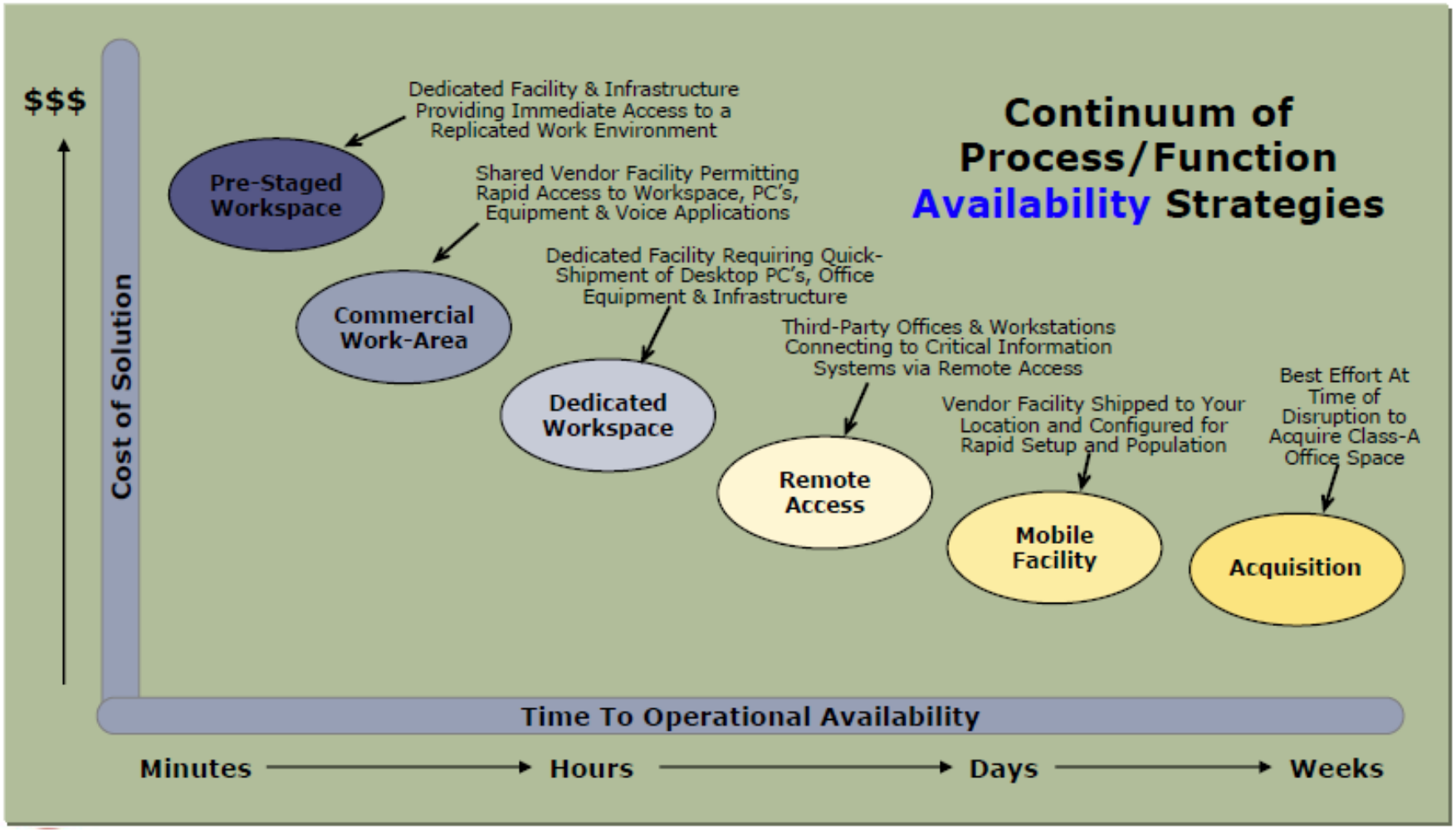
Match the tools to the business needs



Stage 3: strategy development

Process / functions strategies

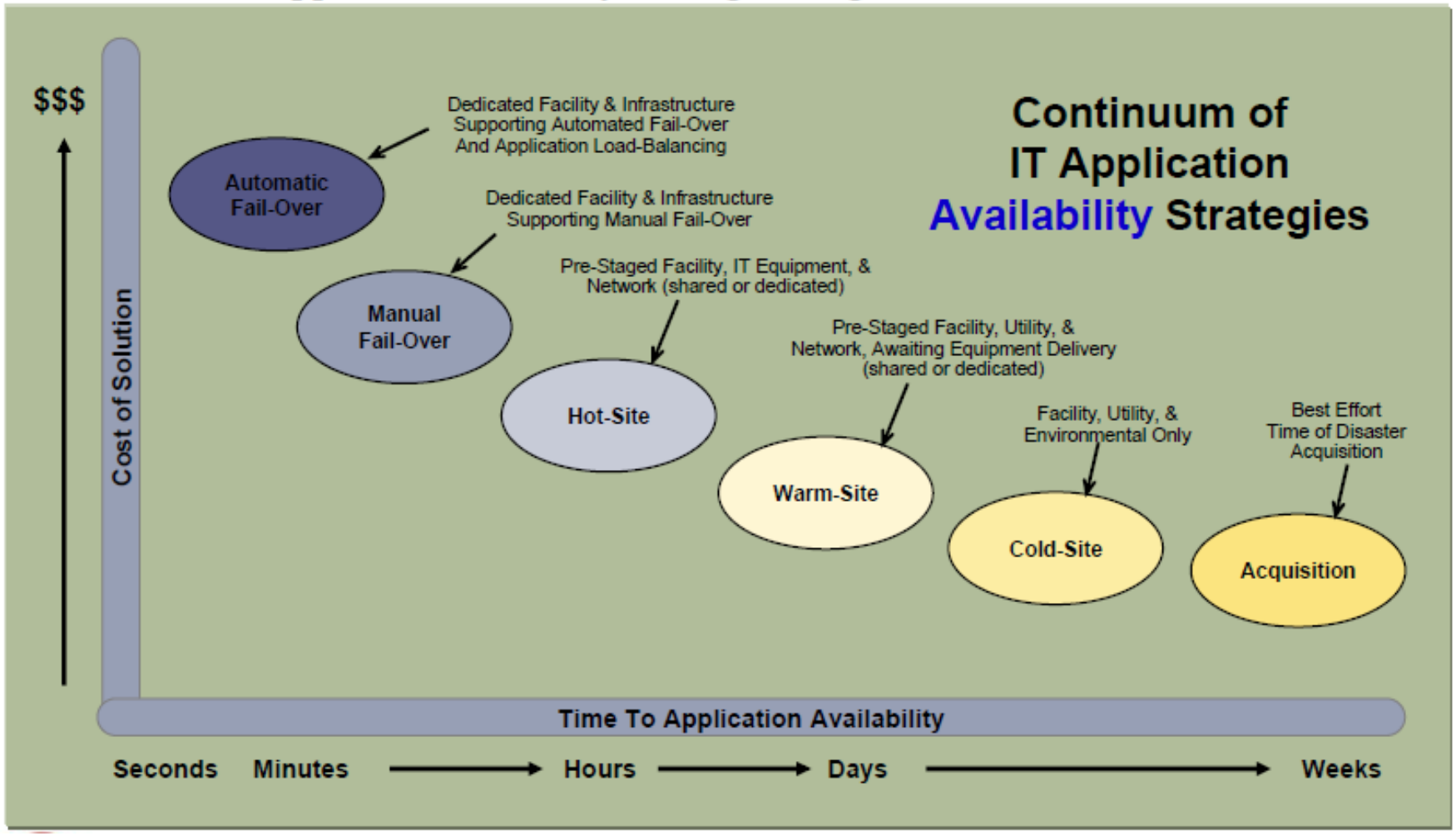
- Alternative functional work-area recovery strategies aligned with RTO.



Stage 3: strategy development

Application availability strategies

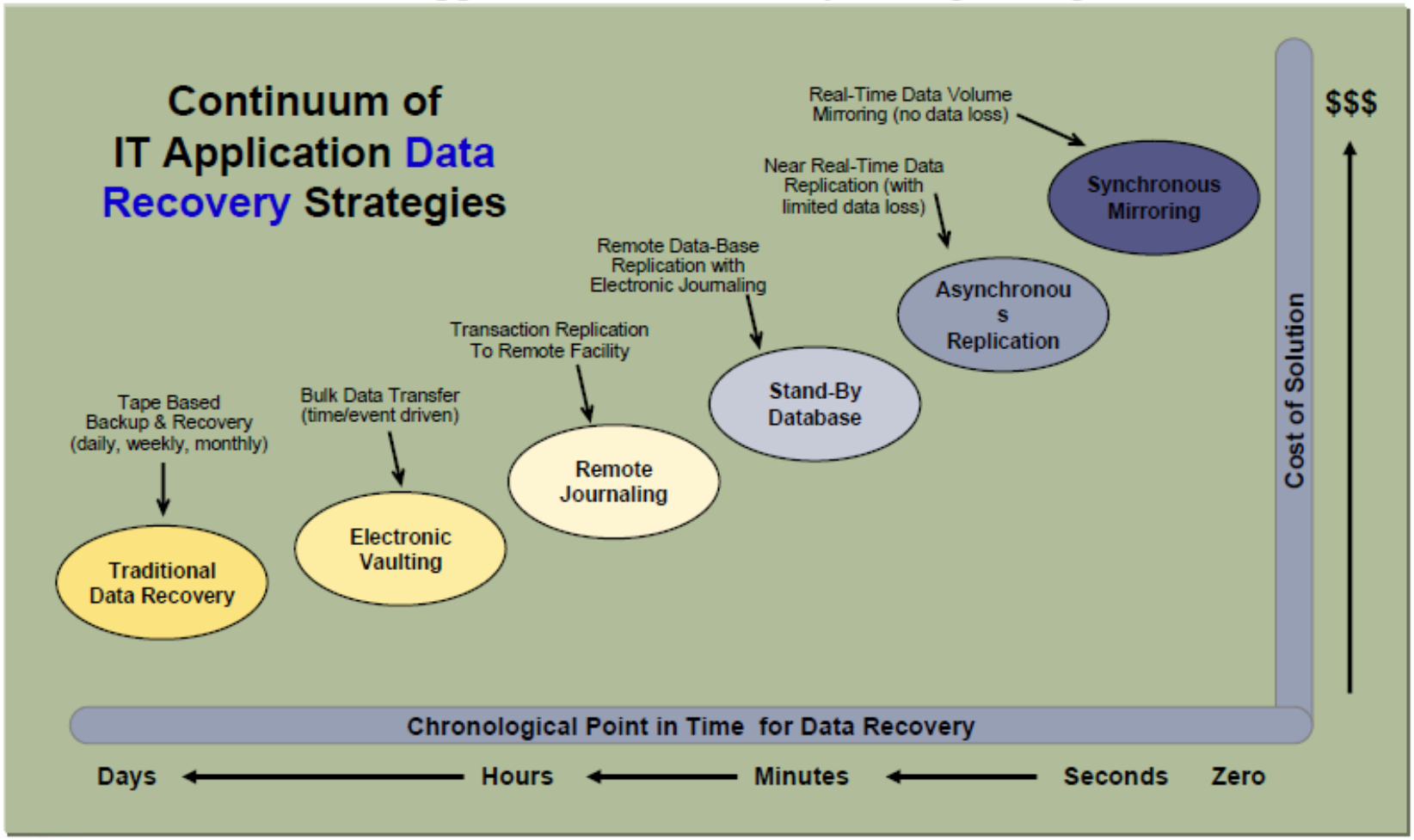
- Alternative IT application recovery strategies aligned with RTO.



Stage 3: strategy development

Application data recovery strategies – selection criteria

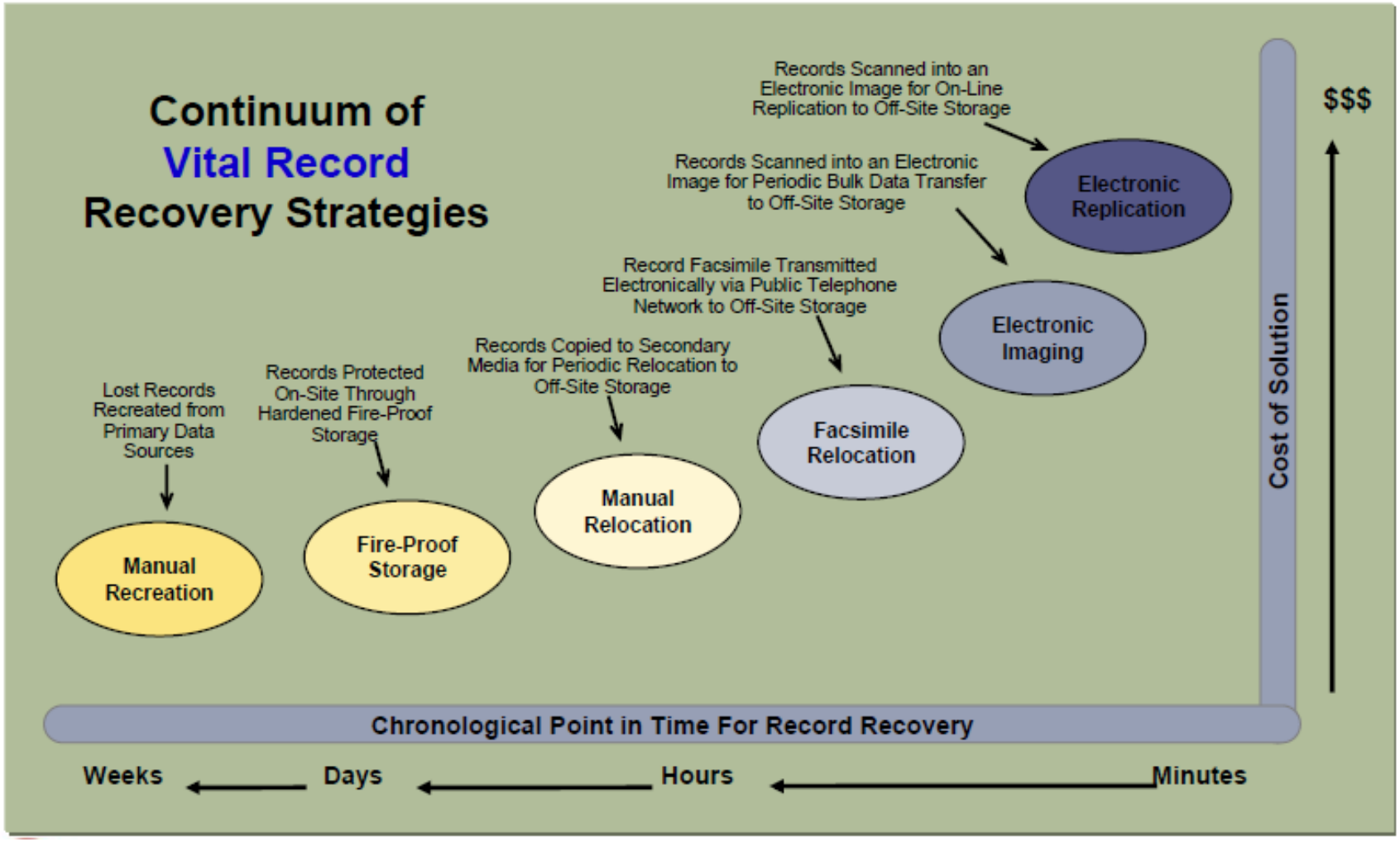
•Alternative electronic application data recovery strategies aligned with RPO.



Stage 3: strategy development

Vital record recovery strategies – selection criteria

- Alternative physical vital record recovery strategies aligned with RPO.

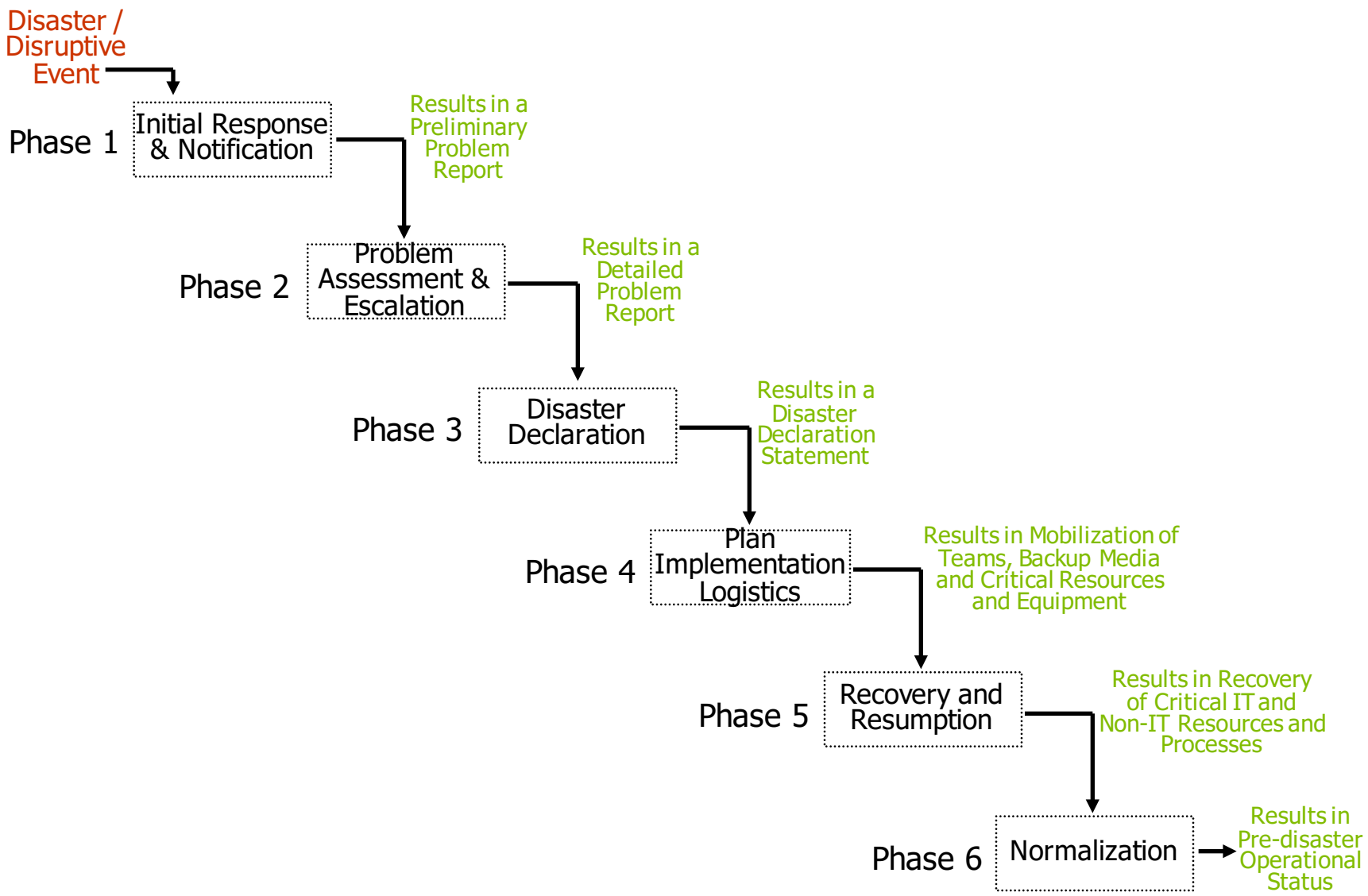


Stage 3: strategy development
Audit issues

- Are the strategies aligned with the RTO / RPO?
- How was the strategy's costs estimated?
- Are the strategies aligned with the management goals?
- Are the strategy's costs well balanced with the amount of the loss?
- Are the strategies easy to maintain, easy to test, easy develop, let to operate for a long time?
- Are the strategy´ selection made by the management?
- Proper documentation

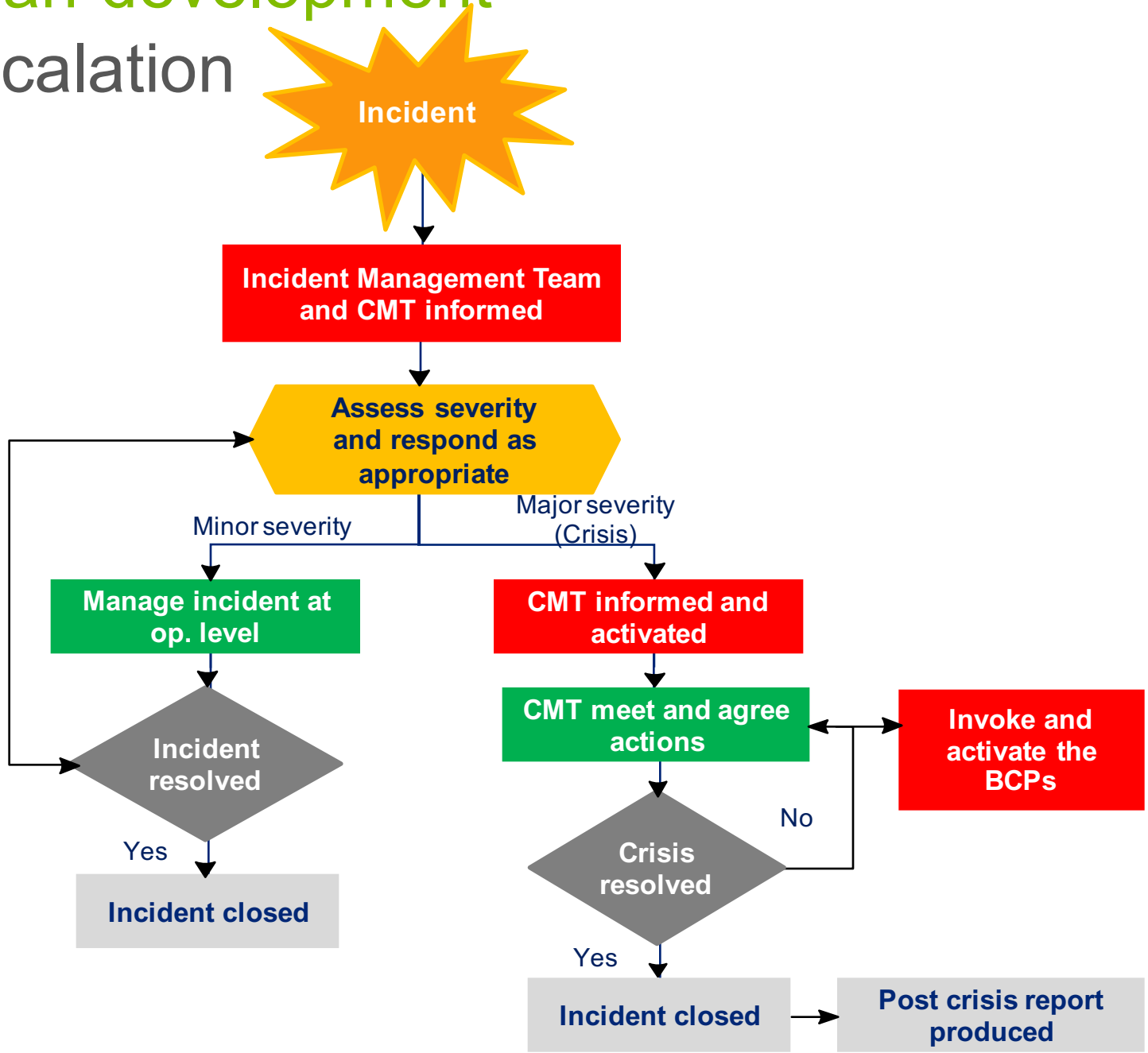
Stage 4: Plan development

Phases



Stage 4: Plan development

Incident escalation



Stage 4: Plan development
Components

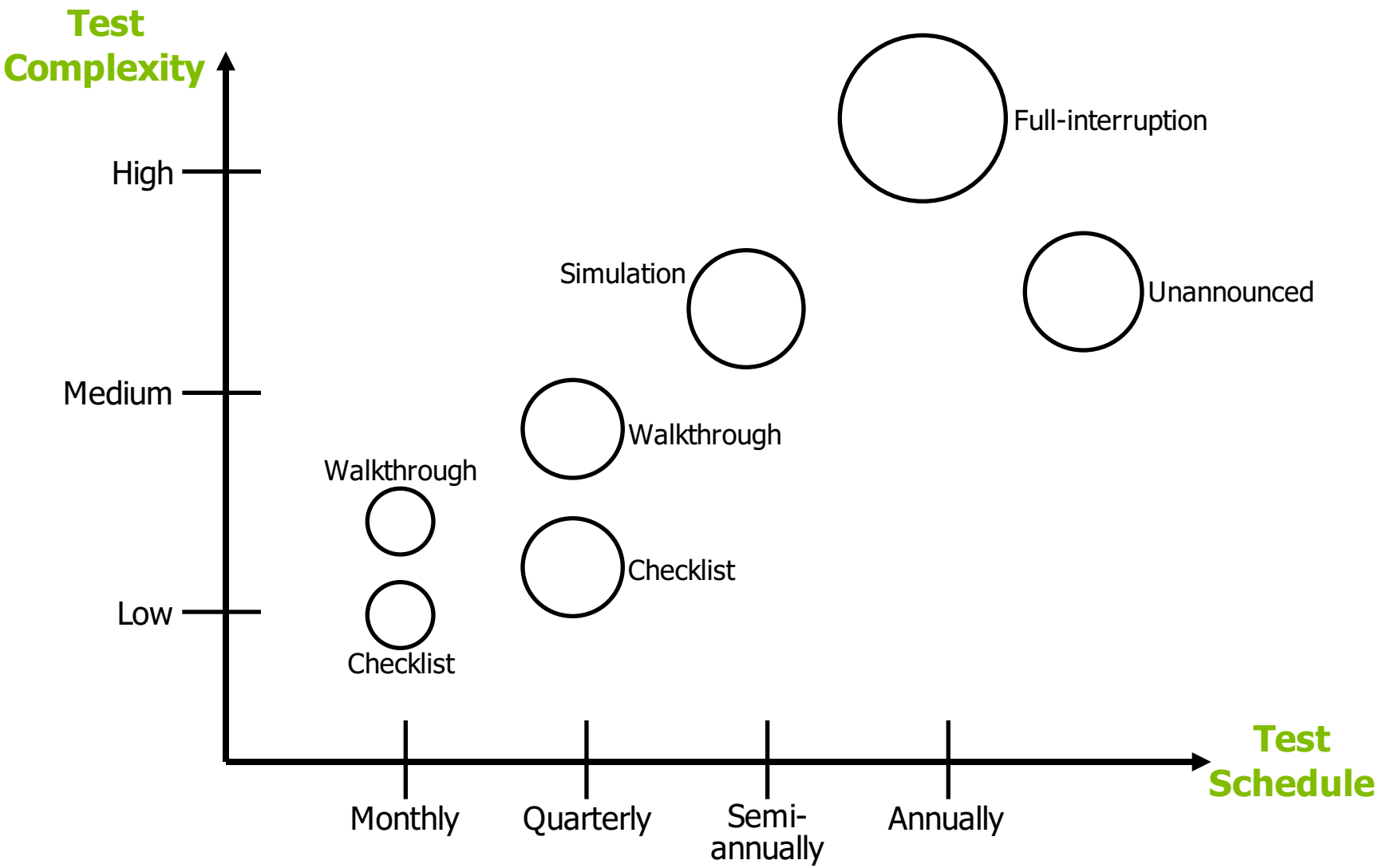
- BCM Policies
- Recovery teams (crisis management team, incident management team, crisis communication team, DRP management team, BCP's teams)
- Governance (BCP leader, DRP Leader)
- Roles and responsibilities (normal and disaster time)
- Key performance indicators (defined and measurement)
- BCP directory (address, cell phone, phone) – internal and external
- Call tree

Stage 4: Plan development
Audit issues

- Are the BCM policies approved by the management?
- Are the incident escalation according with the company's needs and requirements?
- Is properly defined the procedure to share the information of the call tree and directory?
- Are the BCM´s, BCP´s and DRP's leaders properly defined according with the skills and knowledge of the people selected?
- Are the teams well structured?
- Are properly defined the spokesmen?
- Proper documentation

Stage 5: Testing

Testing scheme

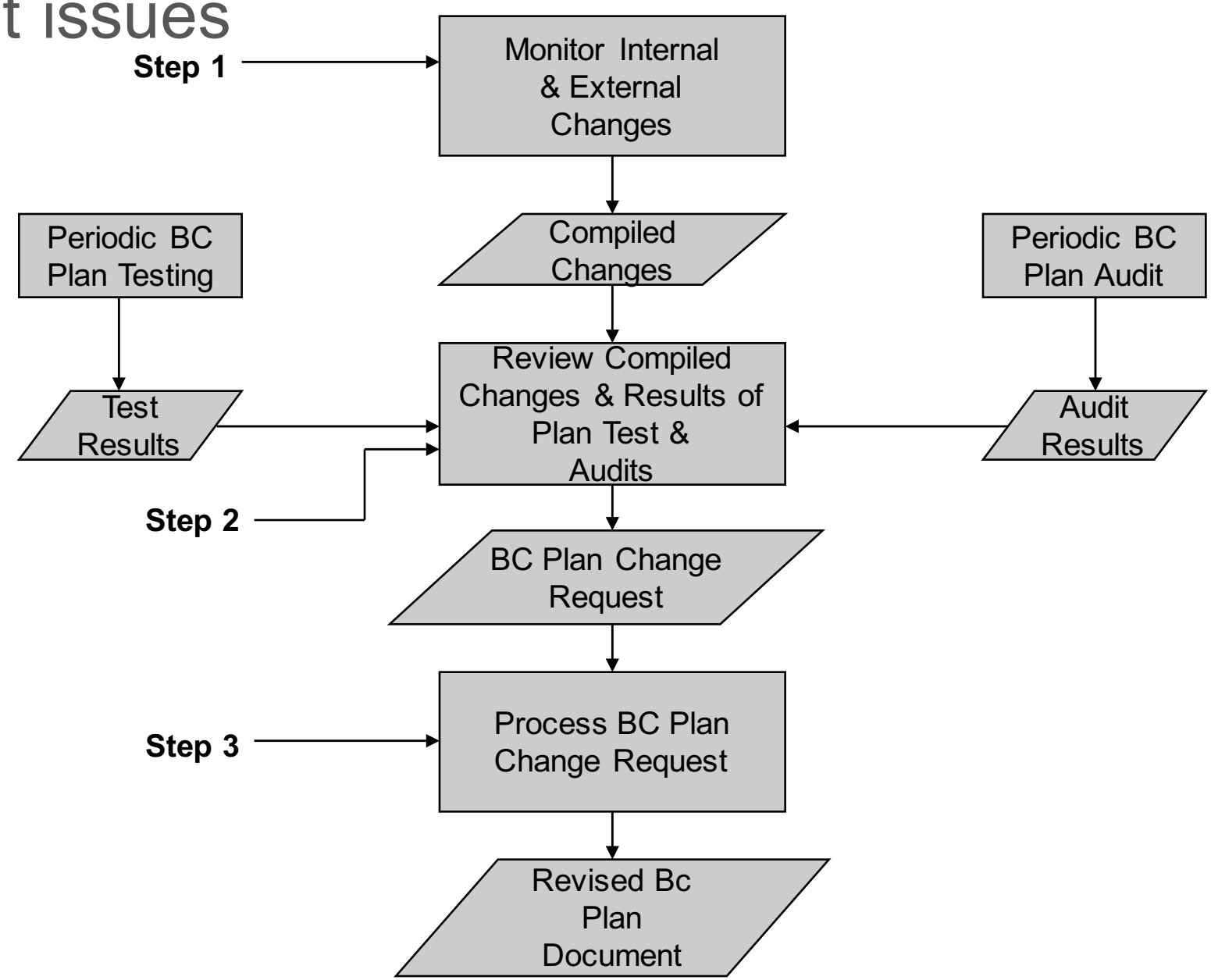


Stage 5: Testing
Audit issues

- Are the BCM's components properly tested?
- Is the BCM's test process properly defined and approved?
- Is the test frequency properly defined?
- Each test has its own data set and time and results expected?
- After each test, the results are analyzed and a work plan is defined to solve the problems presented?
- Is there a follow up to the implementation of the work plan? Who is the responsible?
- Are the strategies aligned with the RTO / RPO?
- Is the test program cumulative?
- Proper documentation

Stage 6: Plan maintenance

Audit issues



Stage 6: Plan maintenance
Audit issues

- Is the BCM's plan maintenance properly defined and approved?
- Are identified the activities that causes bcp changes / modifications?
- Is defined the internal and external BCP audit program?
- Is clear who is the responsible(s) to update the BCP?
- Proper documentation

Thank you