Business Continuity 101

Fairchild Resiliency Systems

fairchild RS™

maestro RS™

Business Continuity

- *Business Continuity (BC) is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.*
  - http://www.thebci.org/index.php/resources/what-is-business-continuity

- Business Continuity is an ongoing set of activities aimed at reducing an organization's risk and improving the organizational ability to respond to and recover from disruptions.

- Organizations that are established for philanthropic purposes, governmental organizations, and other organizations established for purposes other than business will refer to their efforts to mitigate risk and to respond to or recover from disruption as the Continuity of Operations (COOP), rather than "Business Continuity".

Business Continuity

- There are multiple disciplines within Business Continuity:
  - Incident Management
  - Crisis Management
  - Disaster Recovery
  - Pandemic Planning

- *Physical Security* and *Information Security* are sometimes identified as disciplines within Business Continuity.

Incident Management

- Incident Management begins with the collective activities from the initial discovery of a potentially unsafe and/or disruptive situation and the assessment of the situation and selection of a strategy to ensure safety.

- Incident Management includes the detection, escalation, and assessment of the situation.

- Incident Management also includes strategy implementation, monitoring of the situation, and reporting on progress.

The ultimate goal of incident management is to ensure physical safety.

fairchild RS™

Crisis Management

- Crisis Management is the supervisory level administration of the response, recovery, and restoration of normal organizational activities.
- A Crisis Management Team typically consists of upper-level management personnel.
- The Crisis Management team determines the ultimate direction and the selection of strategic initiatives applied to combat the negative impact of a disruption.
- Crisis Management methodology should be applied when an organization is faced with a physical threat such as a hurricane, fire, or flood.
- Crisis Management methodology should also be applied when non-physical threats occur, such as a potential risk to the reputation of the organization.

Disaster Recovery

- Disaster Recovery is the discipline within Business Continuity that focuses on the protection, recovery, and restoration of an organization’s critical technology systems and data.

- While the loss of key systems and data do not pose a threat to physical safety, Information technology outages can cripple an organization’s ability to provide products and services.

Pandemic Planning

- Pandemic Planning is the discipline within Business Continuity that deals with protecting an organization from a widespread outbreak of disease.

- The strategies and methodologies applied in response to the threat of a pandemic vary widely from those applied in response to natural disasters or the loss of key IT systems and data.

Physical Security

- Physical Security sometimes falls under the heading of Business Continuity.
- Physical security is related to the practices and safeguards put into place to prevent and manage physical intrusions into organization facilities.

fairchild RS™

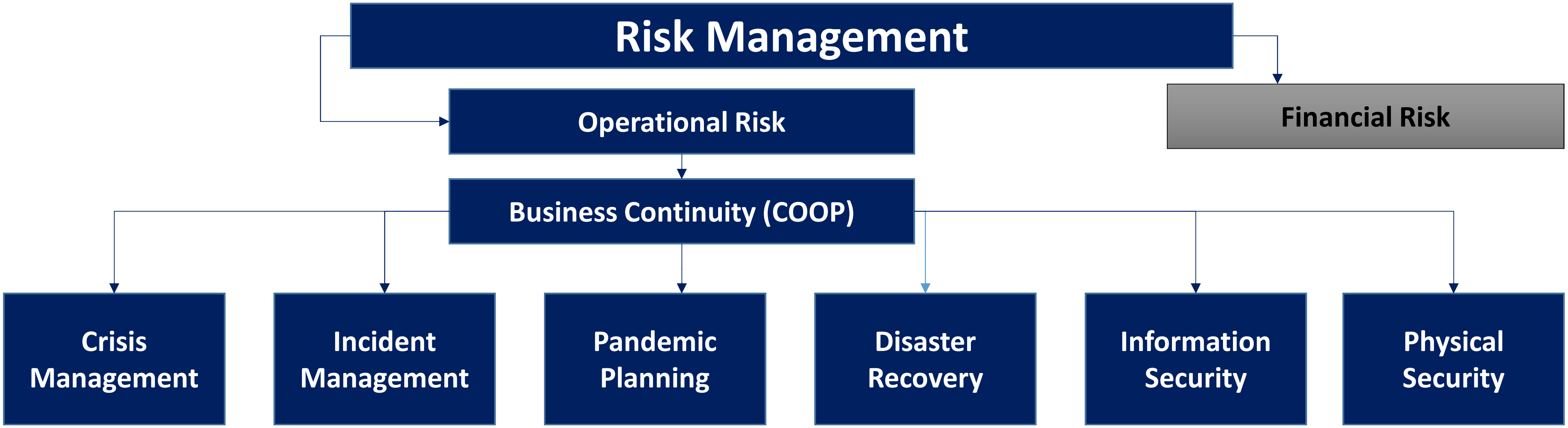
Information Security

- Information Security involves the safeguarding of an organization's IT assets, networks, Intellectual Property (IP), and data.
- In addition to potentially devastating financial consequences, intrusions can also be focused solely on preventing access, destroying data, or compromising an organization by publicizing information.
- Planning for information security is focused on employing preventative measures that restrict access from unauthorized parties and managing breaches when they do occur.
- While the sources of an intrusion are varied and include political groups, the main cause of a breach remains the failure of personnel to follow organizational security guidelines.

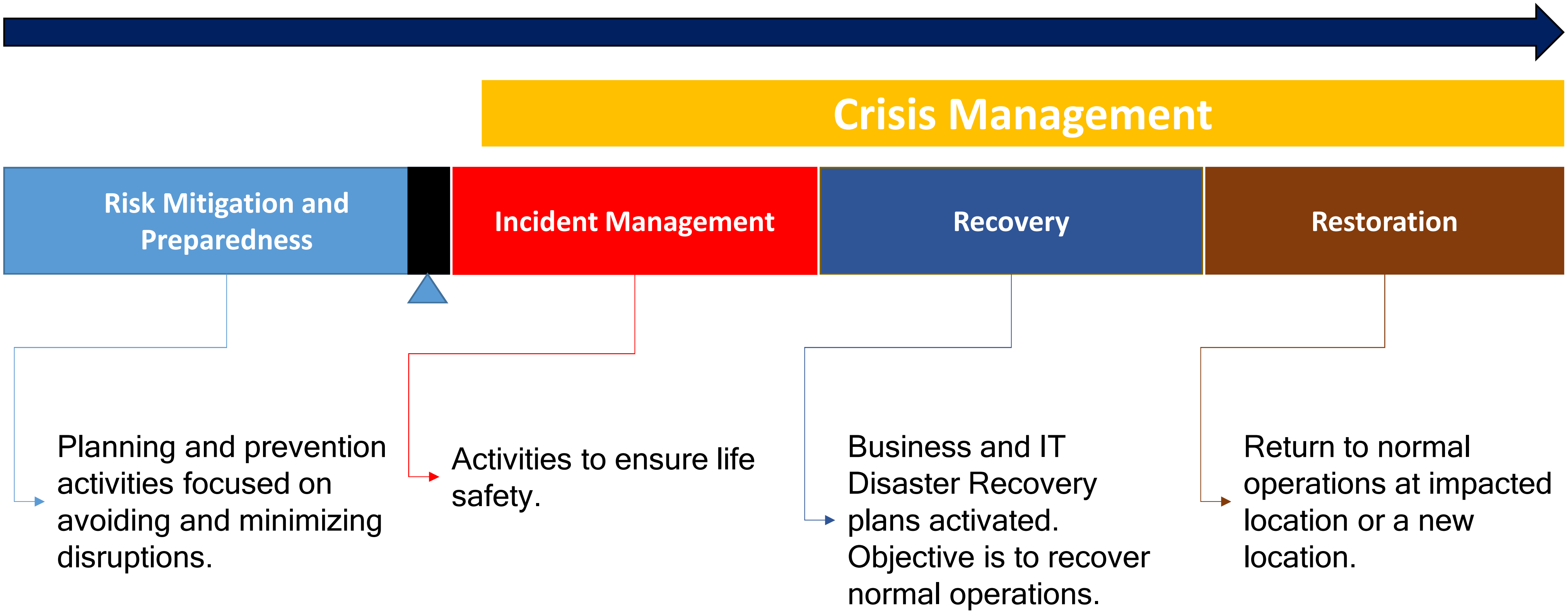
Risk Management

- For most organizations today, Business Continuity falls under the Risk Management department.
- Risk Management is an effort to identify, assess, and prioritize risks to the organization.
- Risk Management puts controls and monitoring mechanisms in place to control the probability and impact of risk.
- There are two major Risk Types:
  - Financial Risk is primarily risk related to an organization’s exposure in markets and its credit risk.
  - Operational Risk is the risk related to organizational procedures.
- Business Continuity falls under Operational Risk.

Typical Risk Management & Business Continuity Structure



Incident Timeline



Crisis Management

Risk Mitigation and Preparedness

Incident Management

Recovery

Restoration

Planning and prevention activities focused on avoiding and minimizing disruptions.

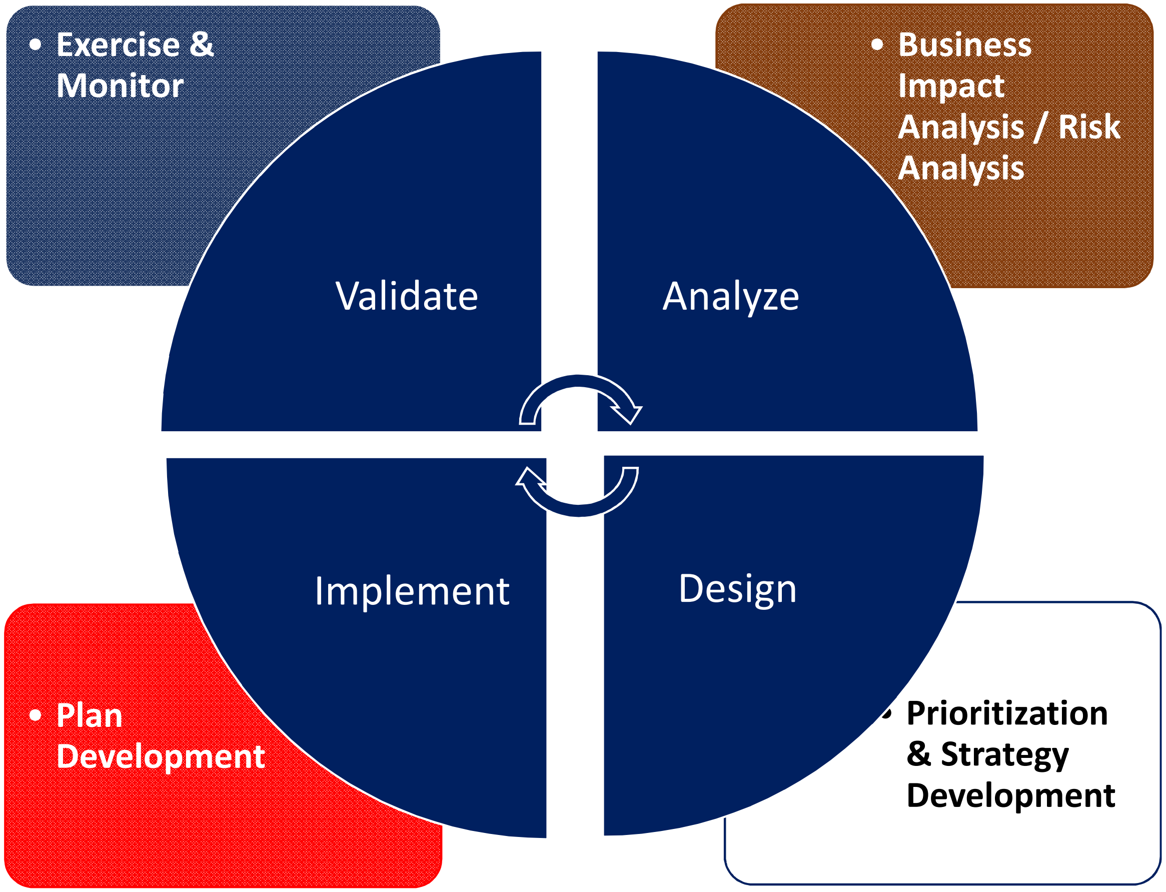
Activities to ensure life safety.

Business and IT Disaster Recovery plans activated. Objective is to recover normal operations.

Return to normal operations at impacted location or a new location.

fairchild RS™

Business Continuity Lifecycle



- Exercise & Monitor

- Business Impact Analysis / Risk Analysis

- Plan Development

- Prioritization & Strategy Development

Analyze

- A Business Impact Analysis (BIA) measures the effect of a disruption over time.
- The BIA results should include the Recovery Time Objective (RTO) of each business process.
- The BIA forms the basis of business and IT recovery strategies.

- A Risk Assessment measures the likelihood of a threat and its potential severity.
- The Risk Assessment provides guidance for selecting effective mitigation strategies.

Design

- Prioritization leverages the data gathered from the BIA and provides a sequence for recovery activities should a disruption occur.
- Strategies are chosen and implemented based on data gathered in the analyze phase.
- The strategies selected will guide the development of recovery plans.

- Organizations will determine how to manage the risks illuminated in the analysis phase
- Risk can be Tolerated, Treated, Transferred, or Terminated
  - Tolerated – the risk is not addressed
  - Treated – measures are taken to reduce/remove the risk
  - Transferred – the risk is absorbed by a third party, for example, an insurance company
  - Terminated – the activity posing a risk is no longer undertaken

Implement

- Plans are developed to address each of the business continuity disciplines.
- The data from the BIA and the strategies developed form a baseline for plan development.
- Personnel identified as having specific roles and responsibilities in plans should review the plans carefully and be familiar with any tasks they are expected to perform.

fairchild RS™

Exercise & Monitor

- The plans developed should be reviewed and approved against current business continuity standards.
- Exercises familiarize personnel with plan requirements and strengthen organizational response and recovery capabilities.
- Exercises will illuminate gaps in the plans where additional information or changes should be applied.
- Exercises provide a validation of current strategies. Strategy revision may be necessary if the exercise highlights shortcomings.
- Organization changes should be monitored to determine if strategies and plans need to be revised to reflect updates to organizational operations.

Questions / More Information

- If you have questions on the content of this presentation or regarding Business Continuity, please see our website at www.fairchildrs.com or call us at 888.930.8250.
- For more information about FairchildApp, visit www.fairchildrs.com/maestro

fairchild RS™

maestro RS™