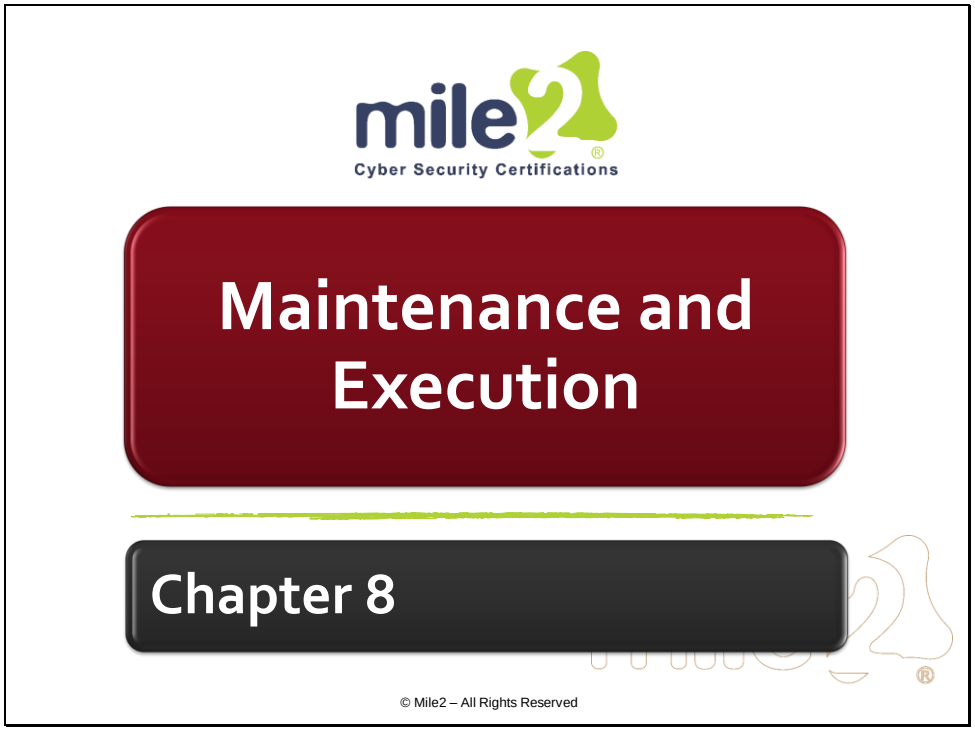
# CDRE - Certified Disaster Recovery Engineer

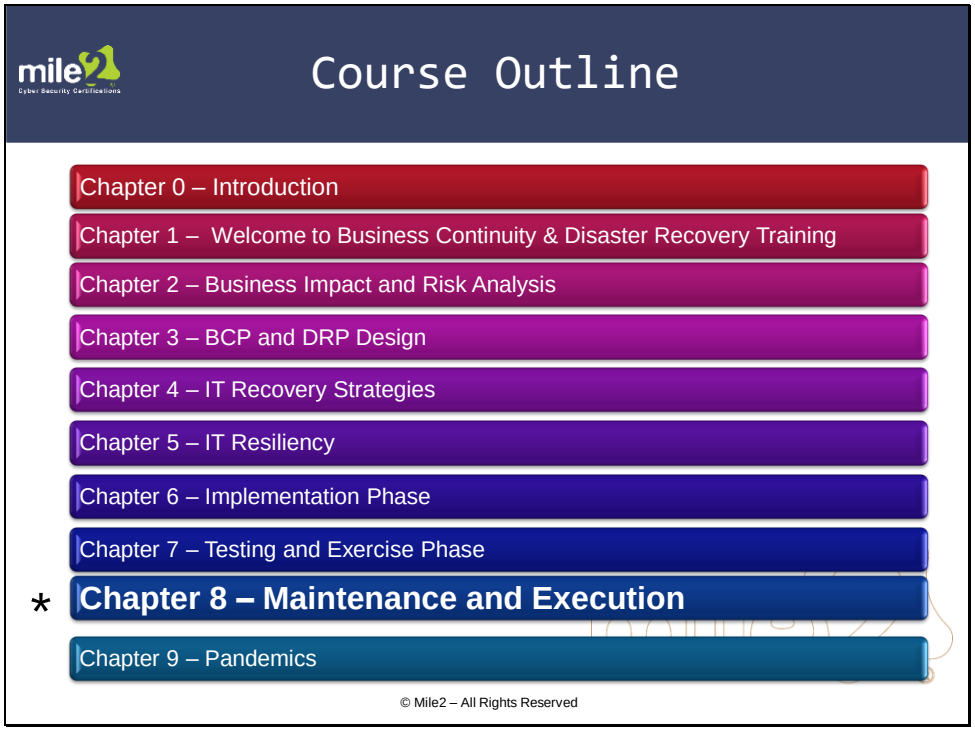
## Chapter 8 - Maintenance and Execution

# WORKBOOK

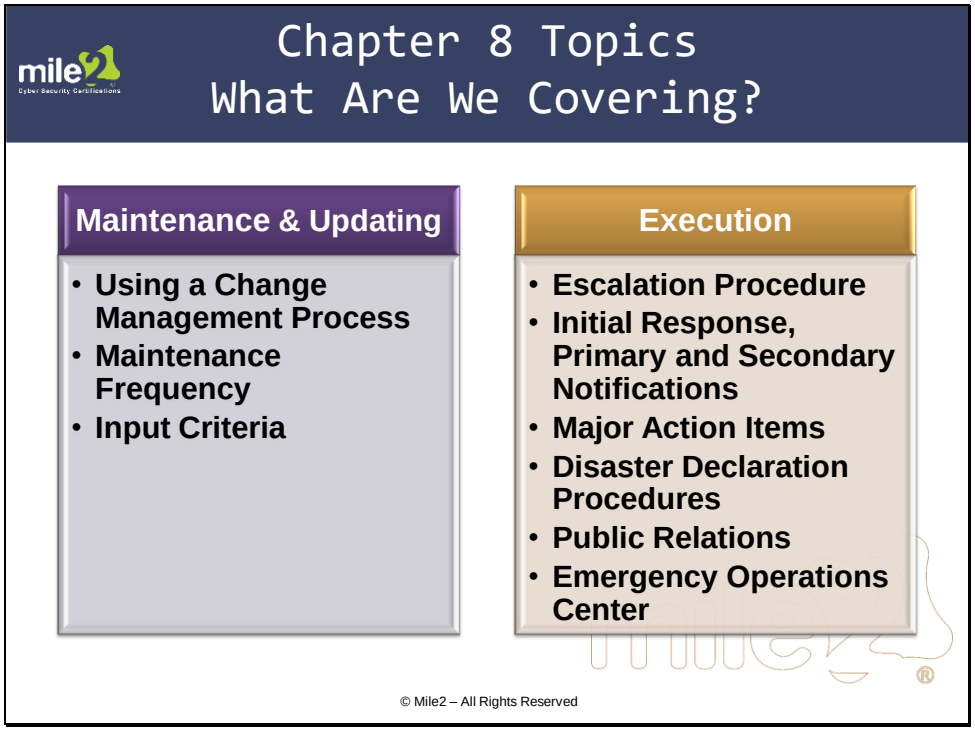
Slide 1


mile2
Cyber Security Certifications
Maintenance and Execution
Chapter 8
© Mile2 – All Rights Reserved

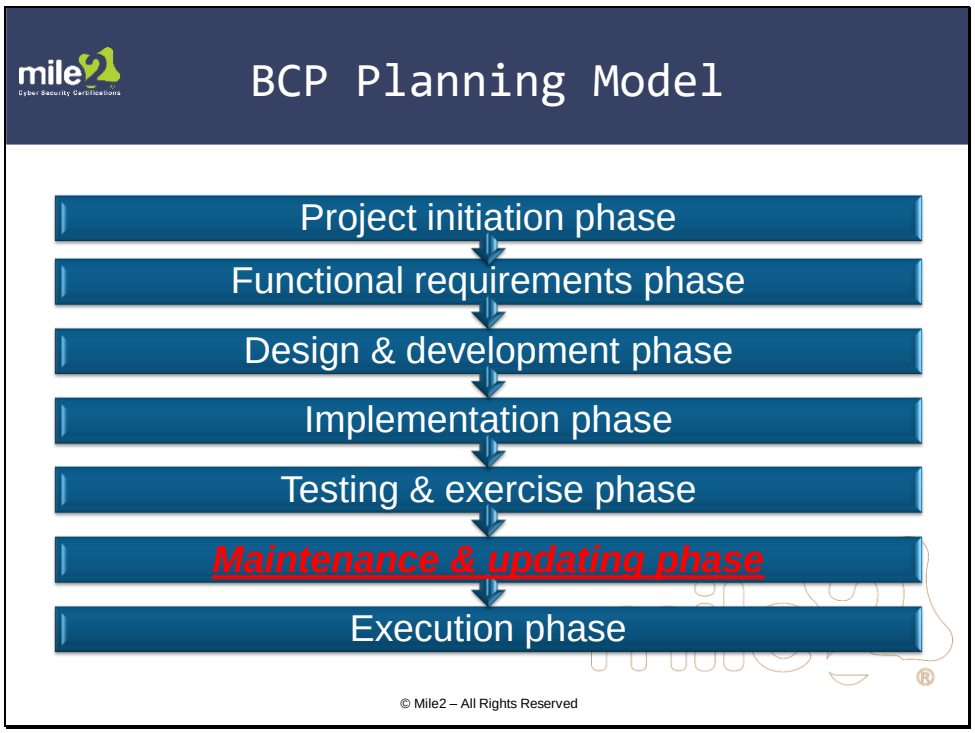
Slide 2


Course Outline
Chapter 0 – Introduction
Chapter 1 – Welcome to Business Continuity & Disaster Recovery Training
Chapter 2 – Business Impact and Risk Analysis
Chapter 3 – BCP and DRP Design
Chapter 4 – IT Recovery Strategies
Chapter 5 – IT Resiliency
Chapter 6 – Implementation Phase
Chapter 7 – Testing and Exercise Phase
*
Chapter 8 – Maintenance and Execution
Chapter 9 – Pandemics
© Mile2 – All Rights Reserved

Slide 3


Chapter 8 Topics
What Are We Covering?
Maintenance & Updating
• Using a Change Management Process
• Maintenance Frequency
• Input Criteria
Execution
• Escalation Procedure
• Initial Response, Primary and Secondary Notifications
• Major Action Items
• Disaster Declaration Procedures
• Public Relations
• Emergency Operations Center
© Mile2 – All Rights Reserved

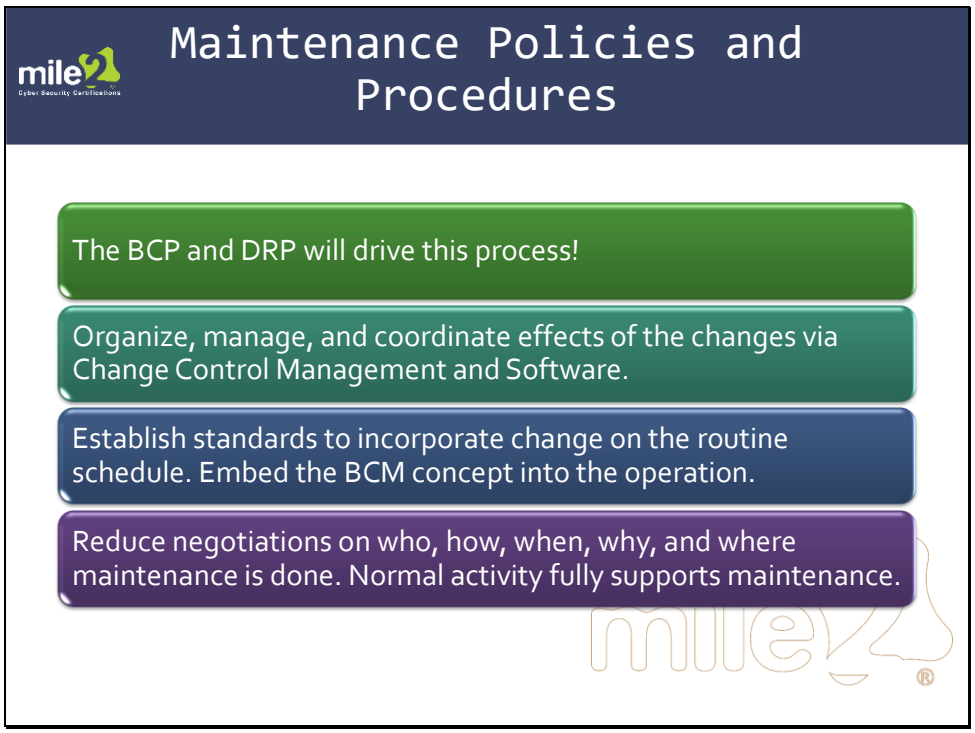
Slide 4


BCP Planning Model
Project initiation phase
Functional requirements phase
Design & development phase
Implementation phase
Testing & exercise phase
Maintenance & updating phase
Execution phase
© Mile2 – All Rights Reserved

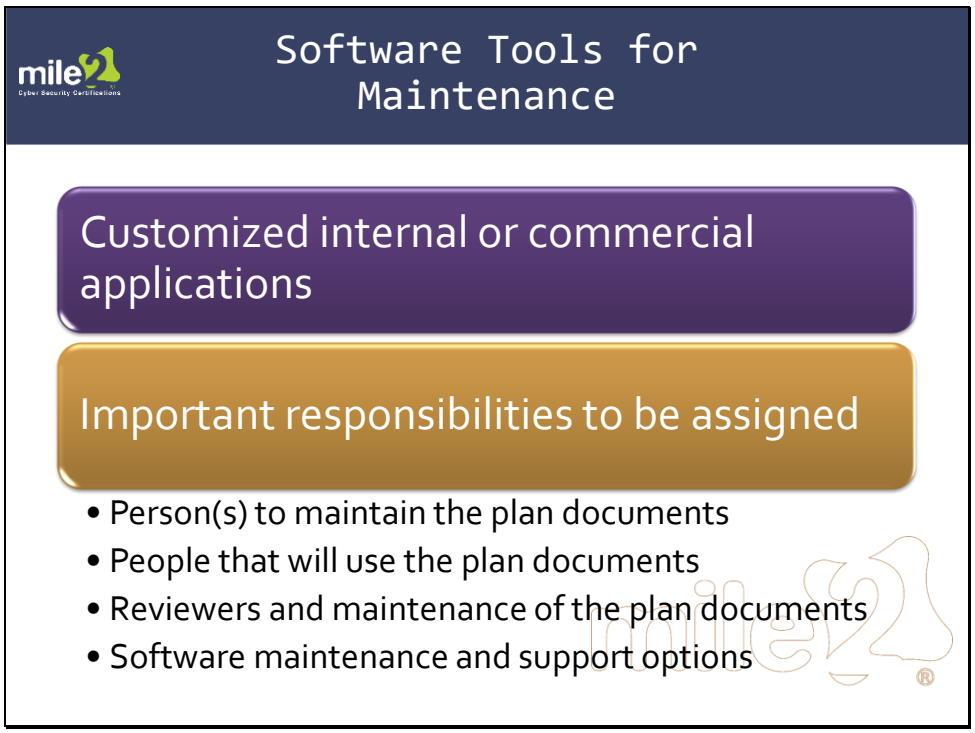
Slide 5

mile2
Cyber Security Certifications
BCP Planning Phases - Maintenance and updating
Section 1
© Mile2 – All Rights Reserved

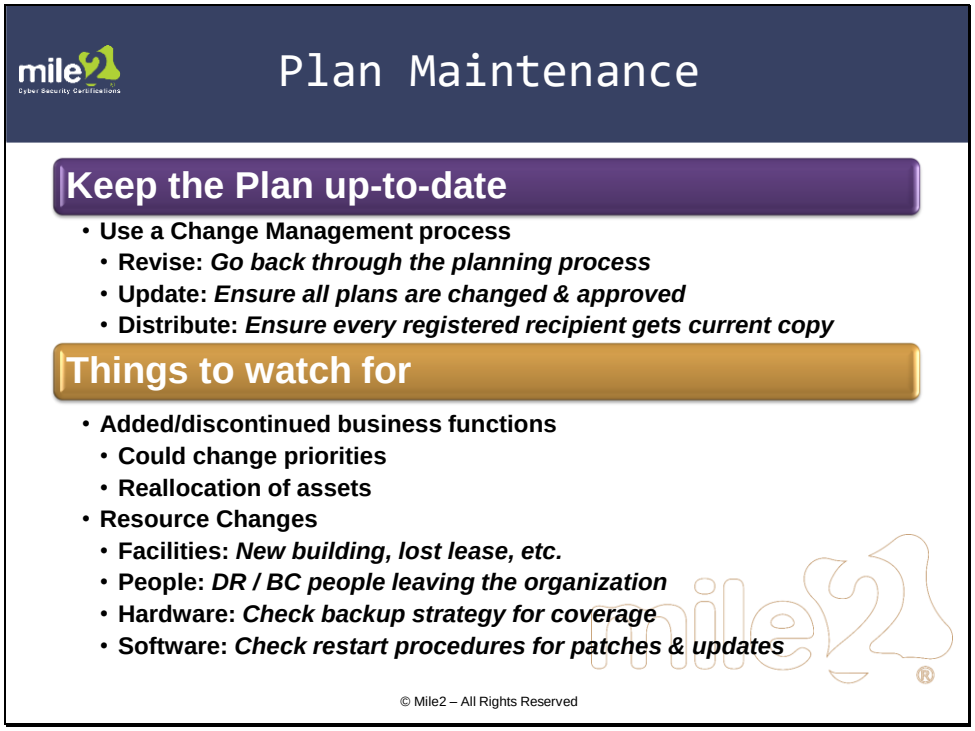
Slide 6


Maintenance Policies and Procedures
The BCP and DRP will drive this process!
Organize, manage, and coordinate effects of the changes via Change Control Management and Software.
Establish standards to incorporate change on the routine schedule. Embed the BCM concept into the operation.
Reduce negotiations on who, how, when, why, and where maintenance is done. Normal activity fully supports maintenance.

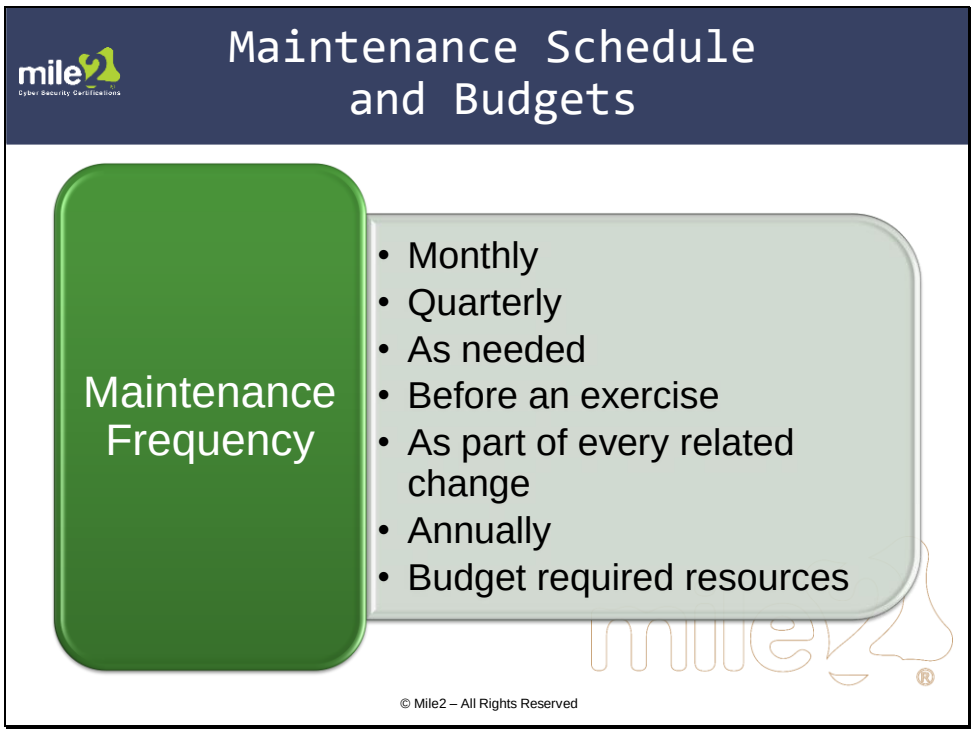
Slide 7


Software Tools for Maintenance
Customized internal or commercial applications
Important responsibilities to be assigned
• Person(s) to maintain the plan documents
• People that will use the plan documents
• Reviewers and maintenance of the plan documents
• Software maintenance and support options

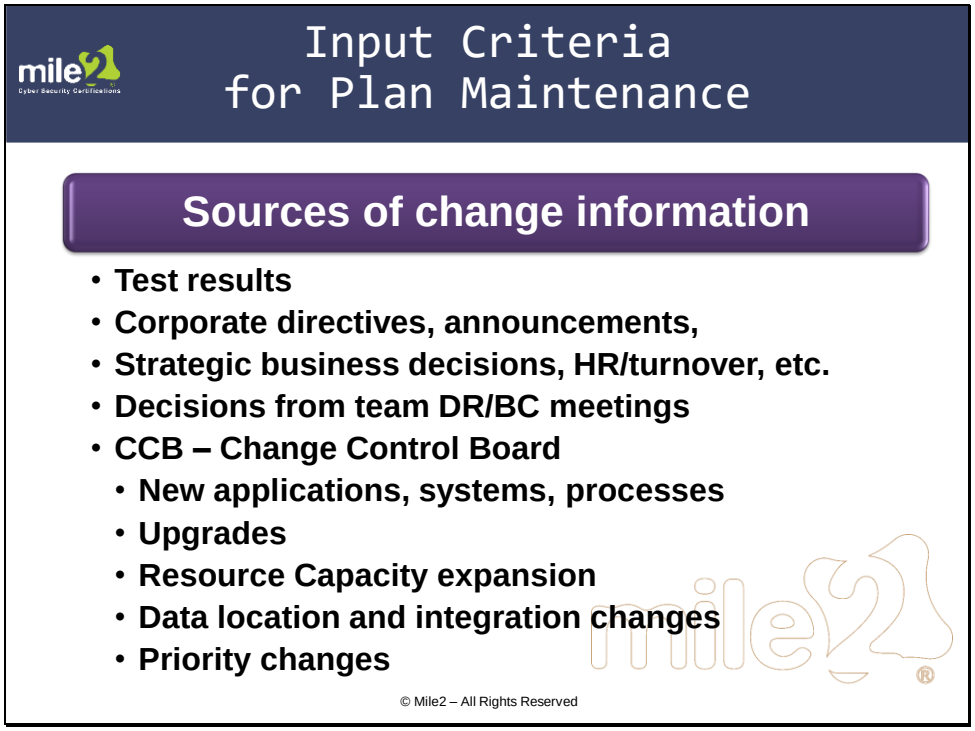
Slide 8


Plan Maintenance
Keep the Plan up-to-date
• Use a Change Management process
• Revise: Go back through the planning process
• Update: Ensure all plans are changed & approved
• Distribute: Ensure every registered recipient gets current copy
Things to watch for
• Added/discontinued business functions
• Could change priorities
• Reallocation of assets
• Resource Changes
• Facilities: New building, lost lease, etc.
• People: DR / BC people leaving the organization
• Hardware: Check backup strategy for coverage
• Software: Check restart procedures for patches & updates
© Mile2 – All Rights Reserved

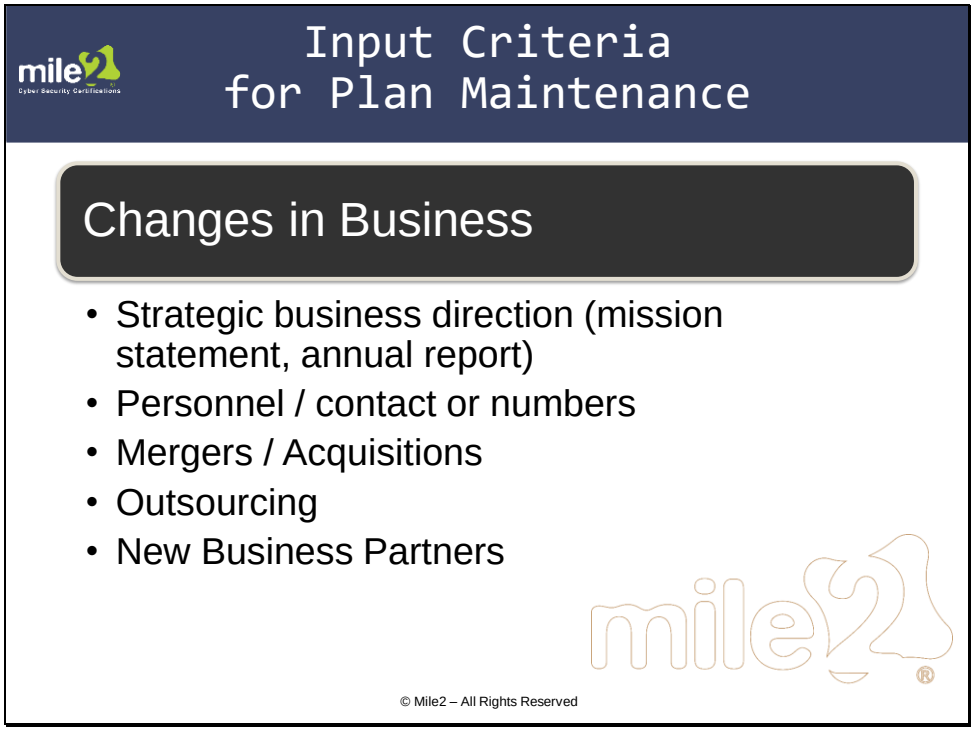
Slide 9


Maintenance Schedule and Budgets
Maintenance Frequency
• Monthly
• Quarterly
• As needed
• Before an exercise
• As part of every related change
• Annually
• Budget required resources
© Mile2 – All Rights Reserved

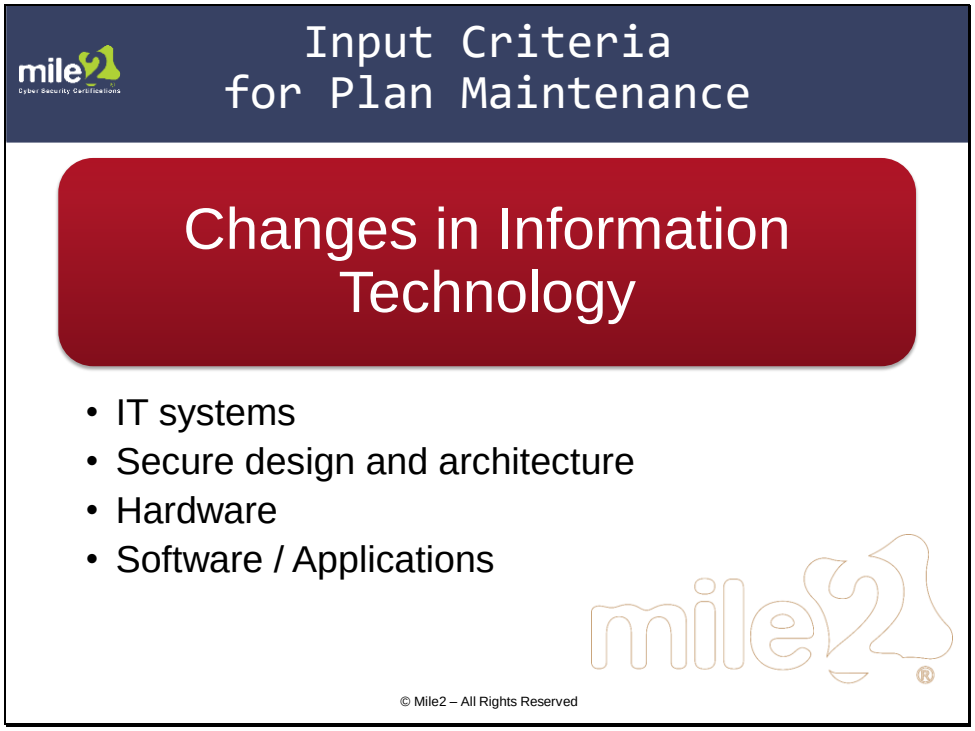
Slide 10


Input Criteria
for Plan Maintenance
Sources of change information
• Test results
• Corporate directives, announcements,
• Strategic business decisions, HR/turnover, etc.
• Decisions from team DR/BC meetings
• CCB – Change Control Board
• New applications, systems, processes
• Upgrades
• Resource Capacity expansion
• Data location and integration changes
• Priority changes
© Mile2 – All Rights Reserved

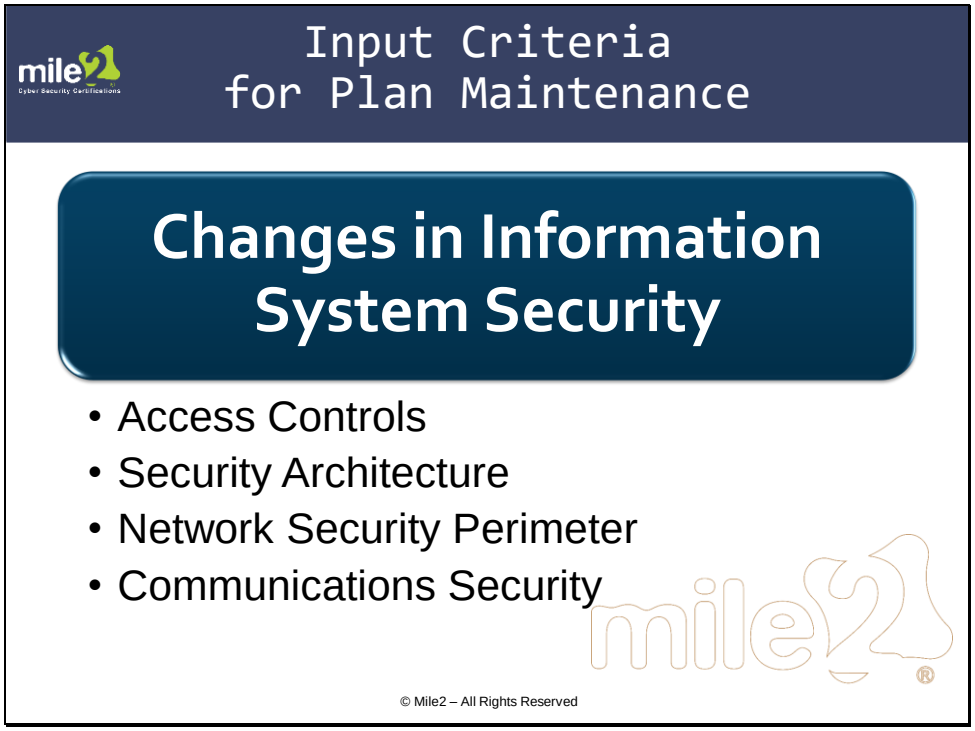
Slide 11


Input Criteria
for Plan Maintenance
Changes in Business
• Strategic business direction (mission statement, annual report)
• Personnel / contact or numbers
• Mergers / Acquisitions
• Outsourcing
• New Business Partners
© Mile2 – All Rights Reserved

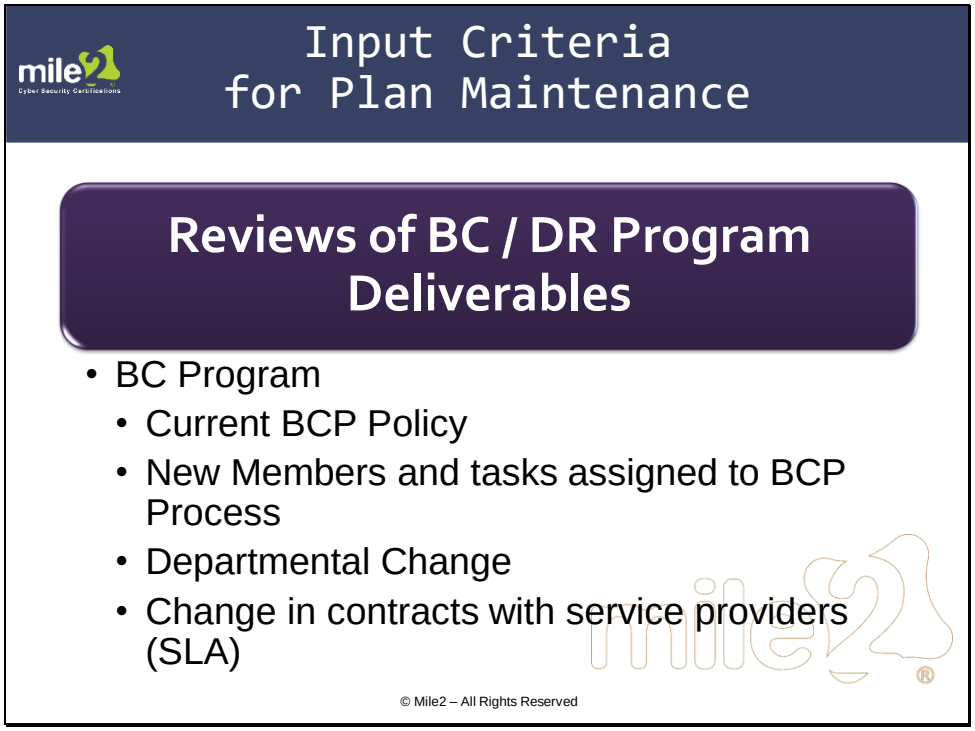
Slide 12


Input Criteria
for Plan Maintenance
Changes in Information Technology
• IT systems
• Secure design and architecture
• Hardware
• Software / Applications
© Mile2 – All Rights Reserved

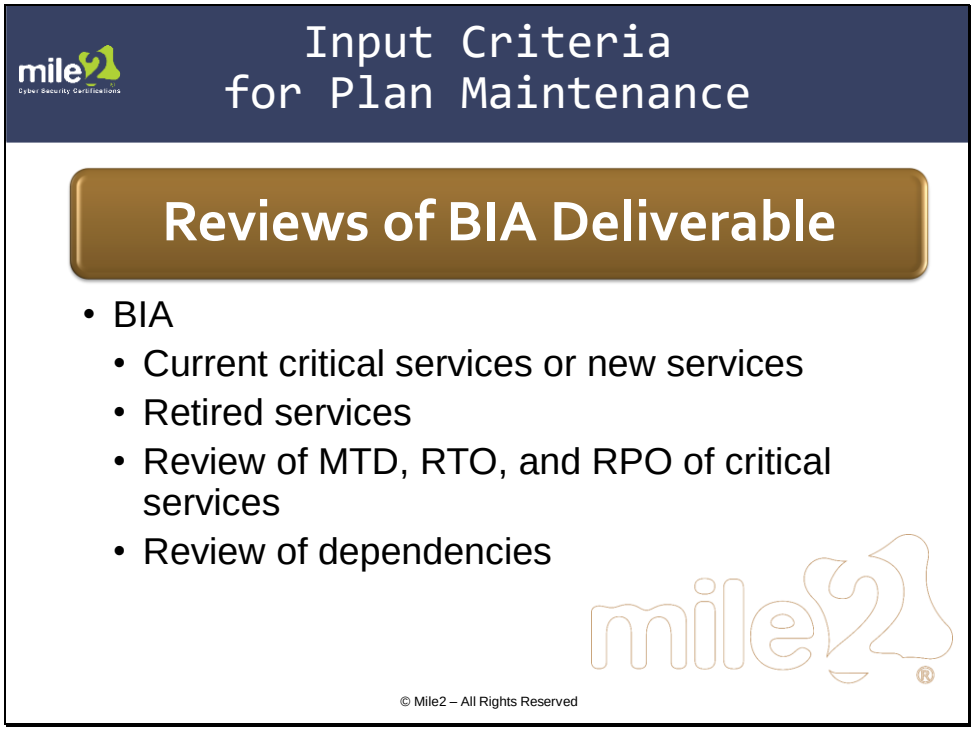
Slide 13


Input Criteria
for Plan Maintenance
Changes in Information System Security
• Access Controls
• Security Architecture
• Network Security Perimeter
• Communications Security
© Mile2 – All Rights Reserved

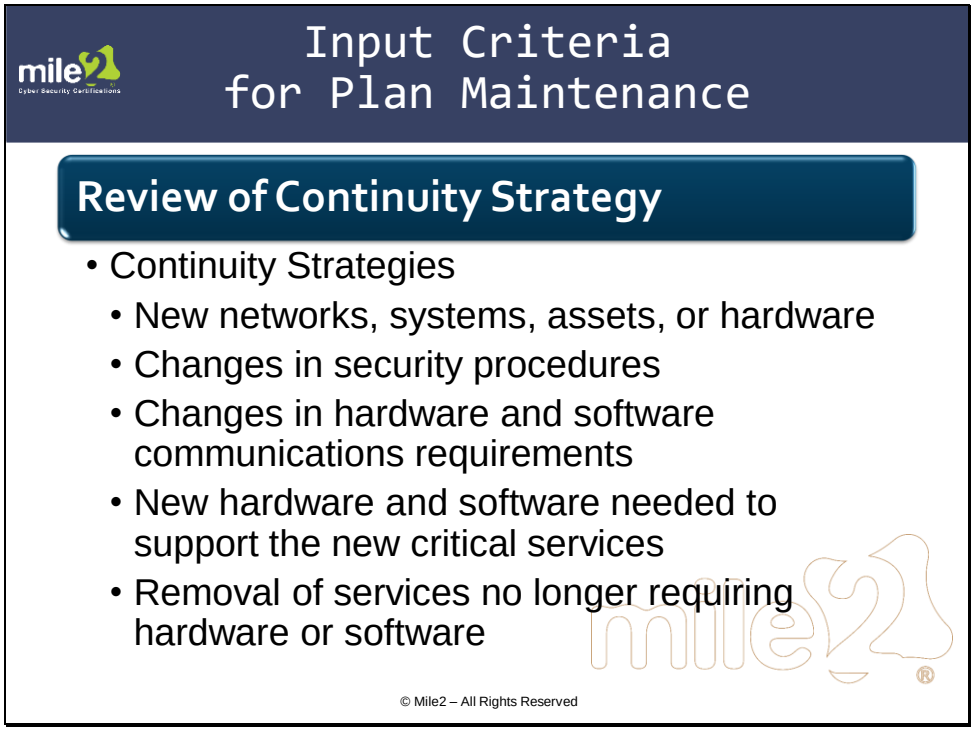
Slide 14


Input Criteria
for Plan Maintenance
Reviews of BC / DR Program Deliverables
• BC Program
• Current BCP Policy
• New Members and tasks assigned to BCP Process
• Departmental Change
• Change in contracts with service providers (SLA)
© Mile2 – All Rights Reserved

Slide 15


Input Criteria
for Plan Maintenance
Reviews of BIA Deliverable
• BIA
• Current critical services or new services
• Retired services
• Review of MTD, RTO, and RPO of critical services
• Review of dependencies
© Mile2 – All Rights Reserved

Slide 16


Input Criteria
for Plan Maintenance
Review of Continuity Strategy
• Continuity Strategies
• New networks, systems, assets, or hardware
• Changes in security procedures
• Changes in hardware and software communications requirements
• New hardware and software needed to support the new critical services
• Removal of services no longer requiring hardware or software
© Mile2 – All Rights Reserved

Slide 17

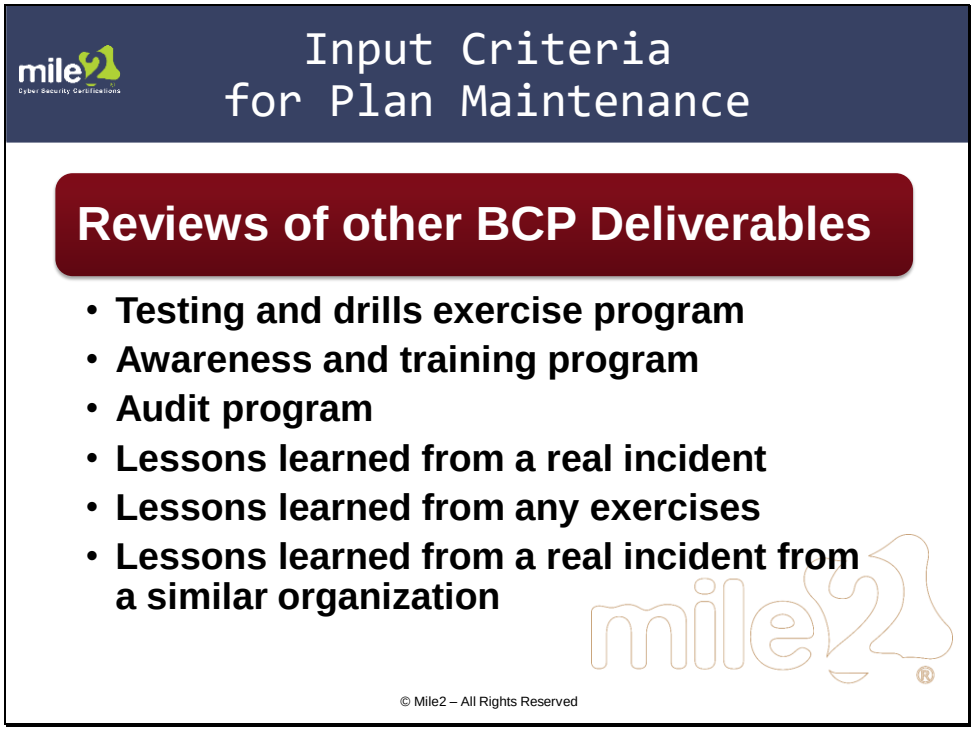
# Input Criteria for Plan Maintenance

## Reviews of BCP and DRP

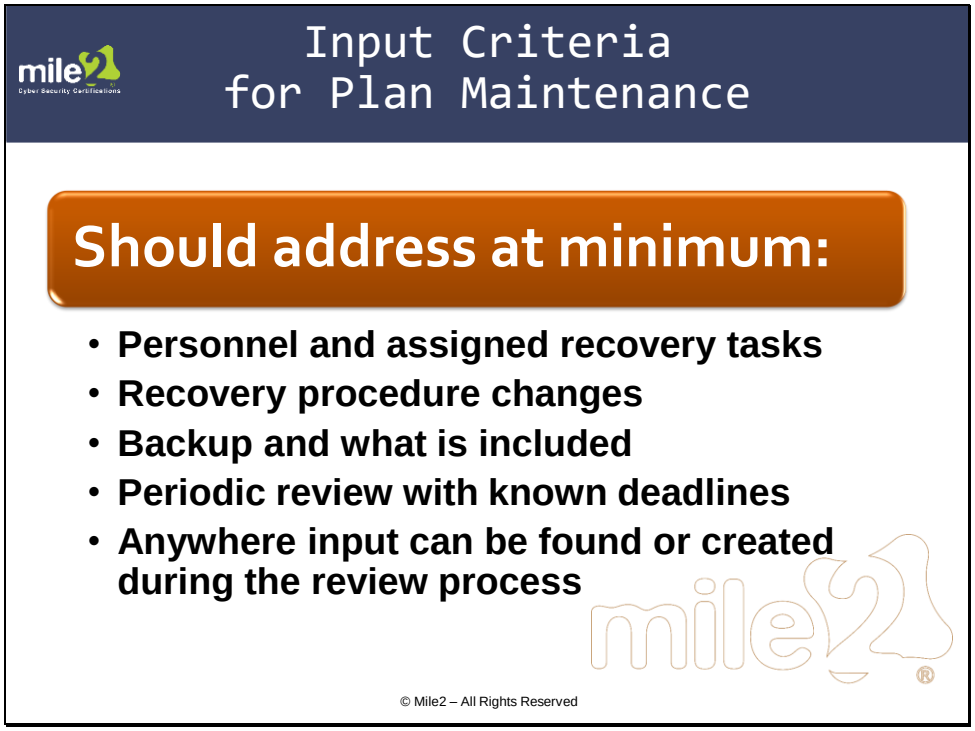
- BC Plan and/or DR Plan results
  - Review of response, recovery, resumption, restoration, and return to home site procedures
    - BC Teams
      - Members
      - Roles and Responsibilities
      - Action Items
    - Notification Lists
      - Alternate Sites
      - List of critical services

© Mile2 – All Rights Reserved

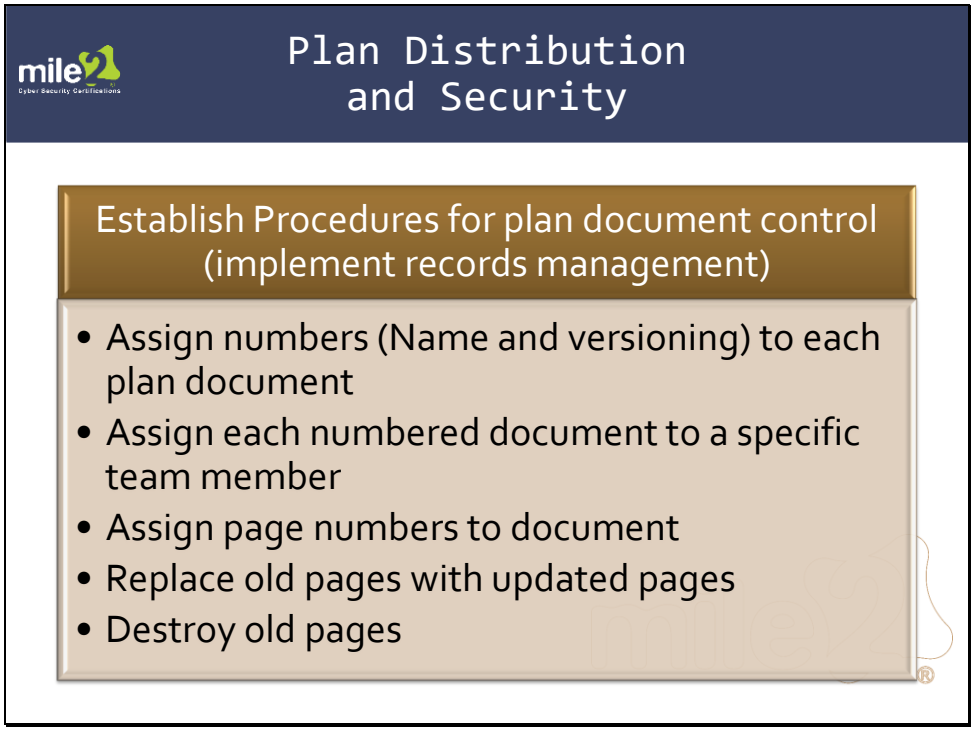
Slide 18


Input Criteria
for Plan Maintenance
Reviews of other BCP Deliverables
• Testing and drills exercise program
• Awareness and training program
• Audit program
• Lessons learned from a real incident
• Lessons learned from any exercises
• Lessons learned from a real incident from a similar organization
© Mile2 – All Rights Reserved

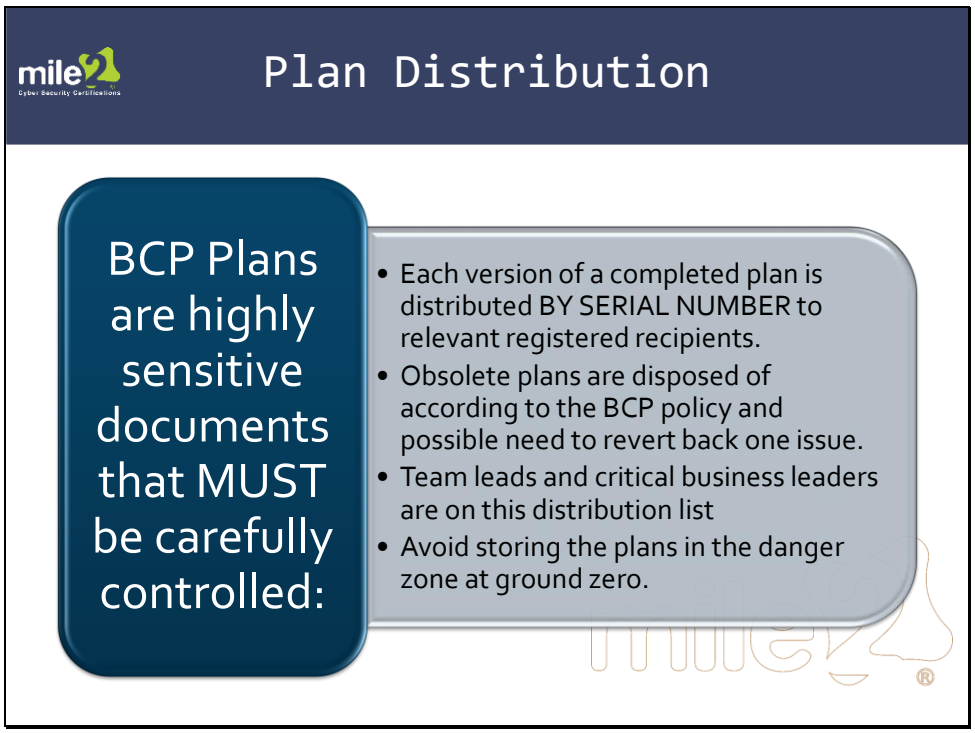
Slide 19


Input Criteria
for Plan Maintenance
Should address at minimum:
• Personnel and assigned recovery tasks
• Recovery procedure changes
• Backup and what is included
• Periodic review with known deadlines
• Anywhere input can be found or created during the review process
© Mile2 – All Rights Reserved

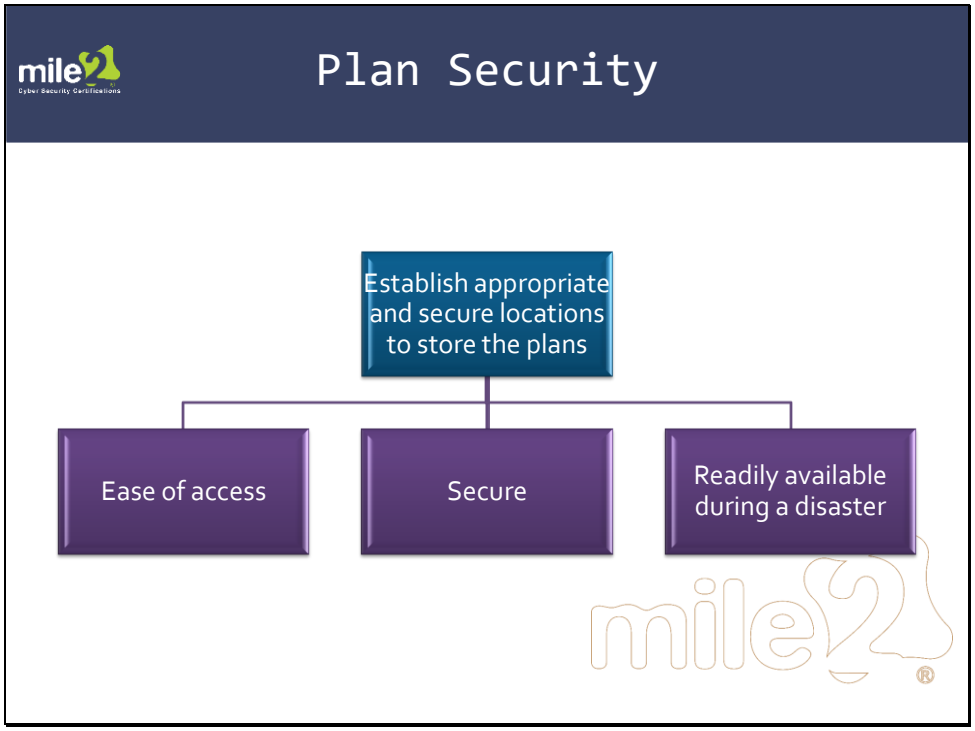
Slide 20


Plan Distribution and Security
Establish Procedures for plan document control (implement records management)
• Assign numbers (Name and versioning) to each plan document
• Assign each numbered document to a specific team member
• Assign page numbers to document
• Replace old pages with updated pages
• Destroy old pages

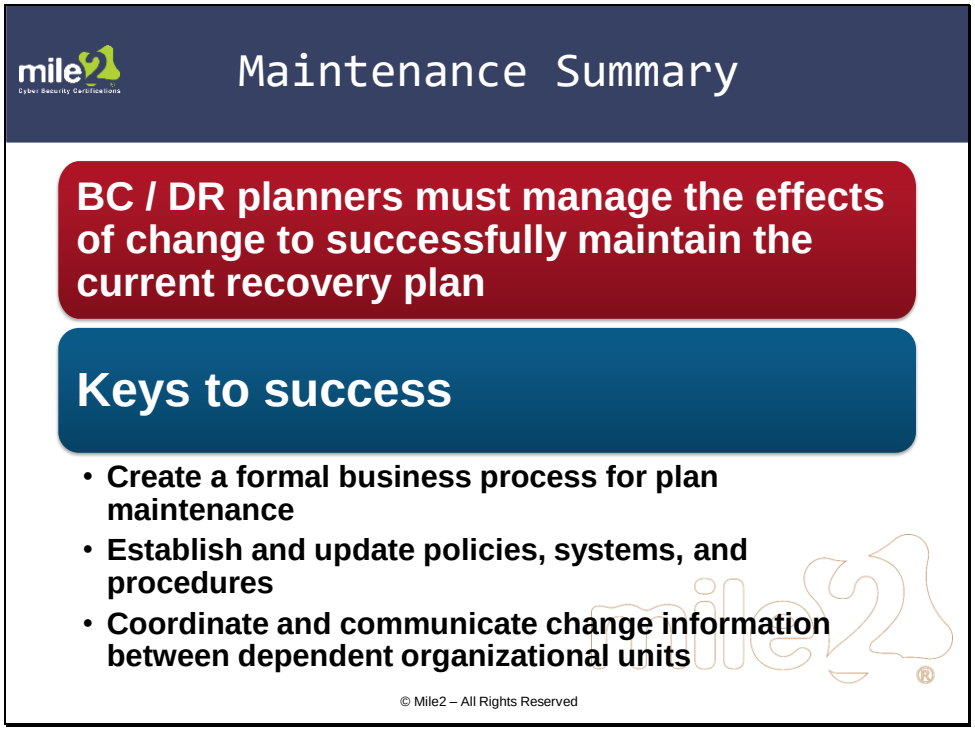
Slide 21


mile2
Cyber Security Certifications
Plan Distribution
BCP Plans are highly sensitive documents that MUST be carefully controlled:
• Each version of a completed plan is distributed BY SERIAL NUMBER to relevant registered recipients.
• Obsolete plans are disposed of according to the BCP policy and possible need to revert back one issue.
• Team leads and critical business leaders are on this distribution list
• Avoid storing the plans in the danger zone at ground zero.

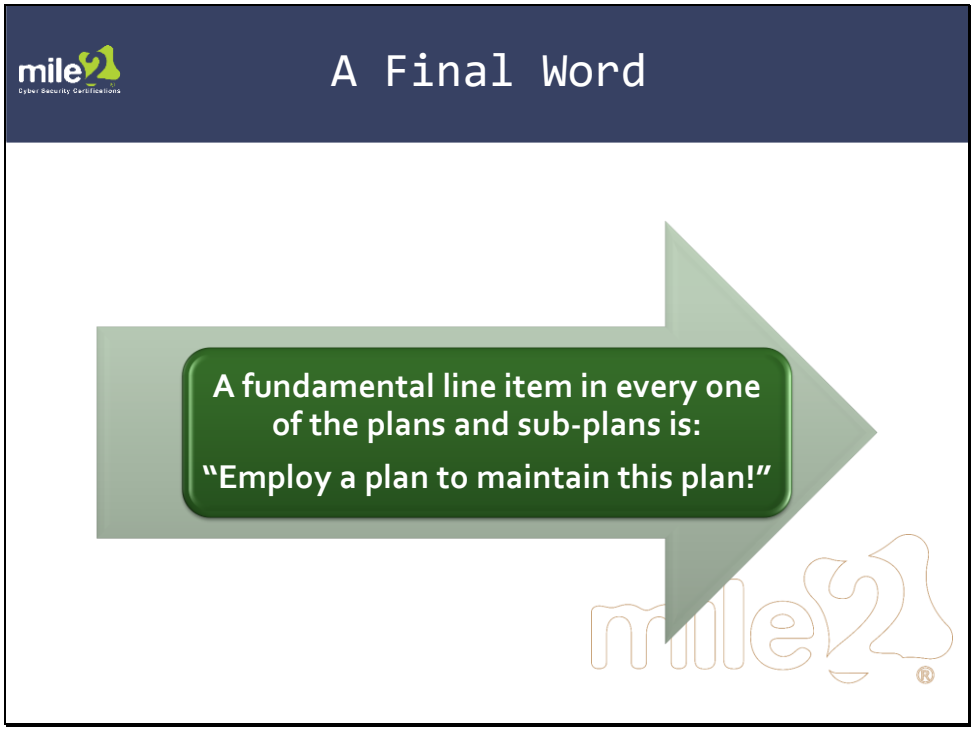
Slide 22


Plan Security
Establish appropriate and secure locations to store the plans
Ease of access
Secure
Readily available during a disaster

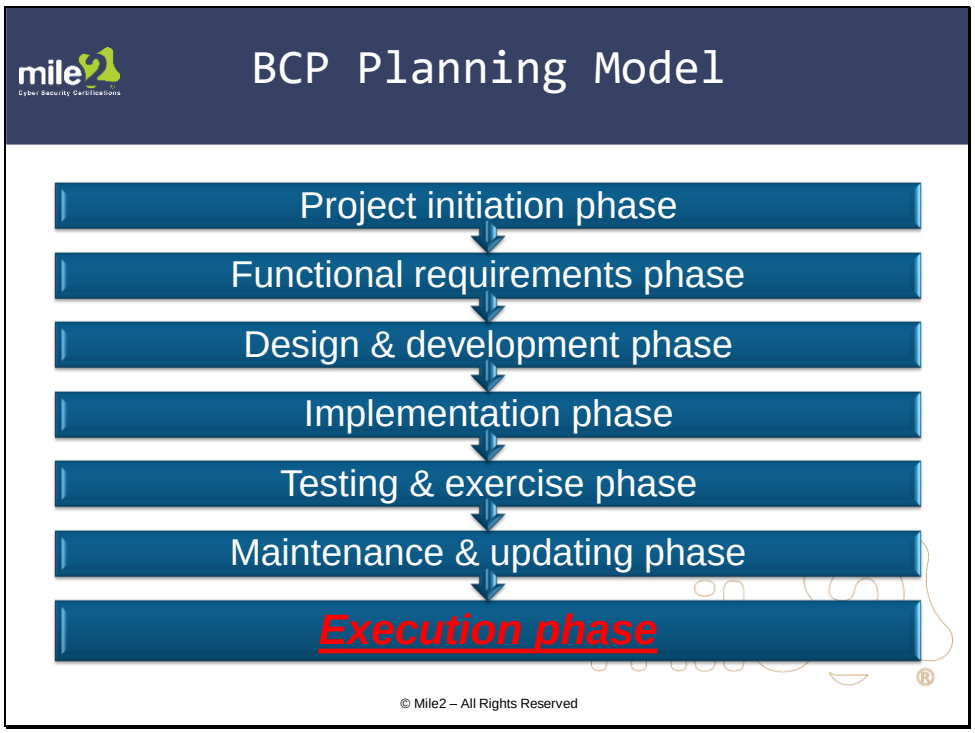
Slide 23


Maintenance Summary
BC / DR planners must manage the effects of change to successfully maintain the current recovery plan
Keys to success
• Create a formal business process for plan maintenance
• Establish and update policies, systems, and procedures
• Coordinate and communicate change information between dependent organizational units
© Mile2 – All Rights Reserved

Slide 24


A Final Word
A fundamental line item in every one of the plans and sub-plans is:
"Employ a plan to maintain this plan!"

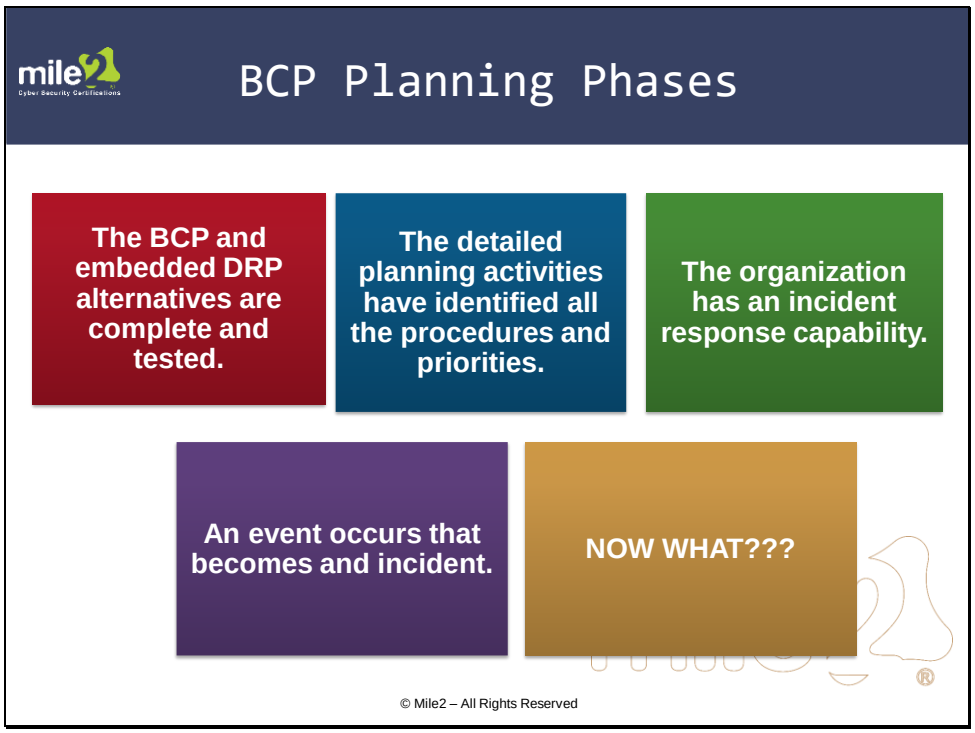
Slide 25


BCP Planning Model
Project initiation phase
Functional requirements phase
Design & development phase
Implementation phase
Testing & exercise phase
Maintenance & updating phase
Execution phase
© Mile2 – All Rights Reserved

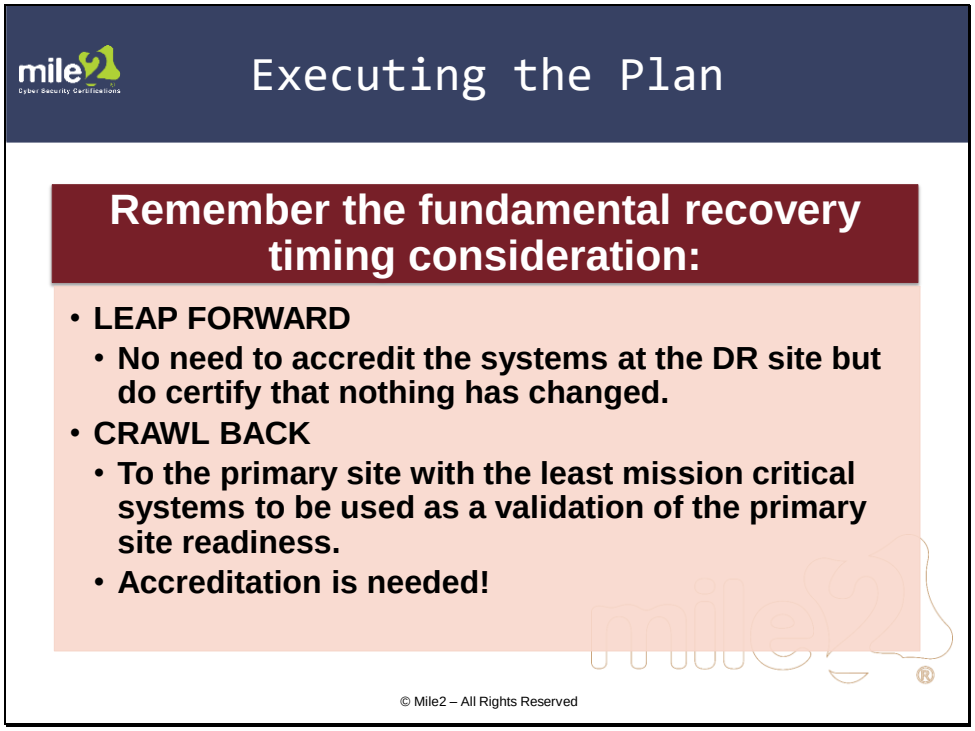
Slide 26

mile2
Cyber Security Certifications
BCP Planning Phases – Execution Phase
Section 2
©Mile2 – All Rights Reserved

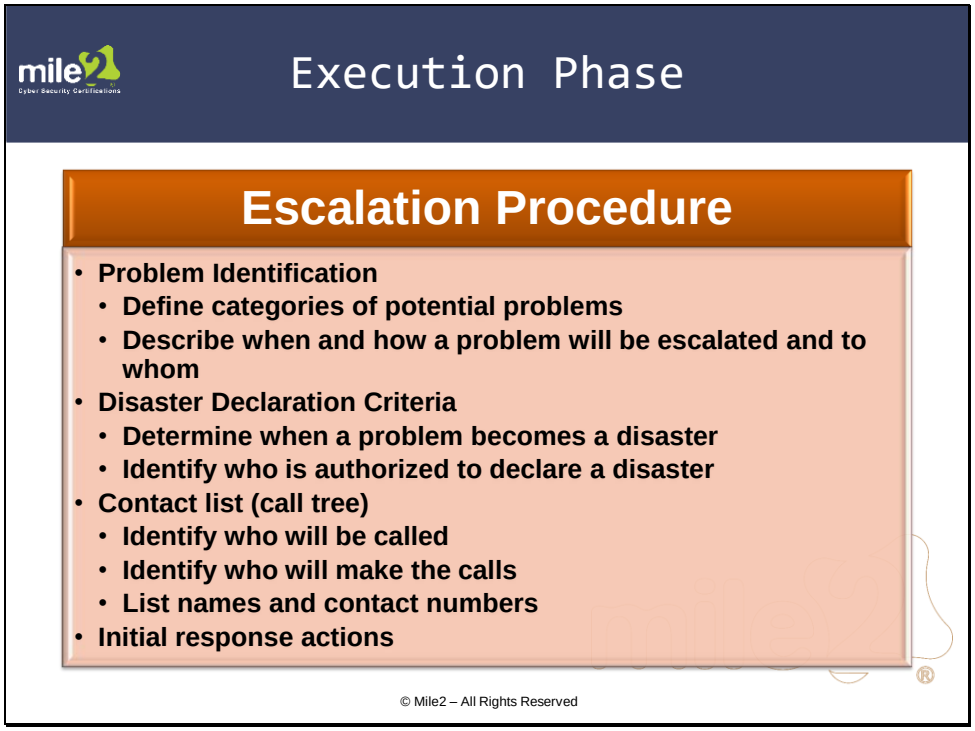
Slide 27


BCP Planning Phases
The BCP and embedded DRP alternatives are complete and tested.
The detailed planning activities have identified all the procedures and priorities.
The organization has an incident response capability.
An event occurs that becomes and incident.
NOW WHAT???
© Mile2 – All Rights Reserved

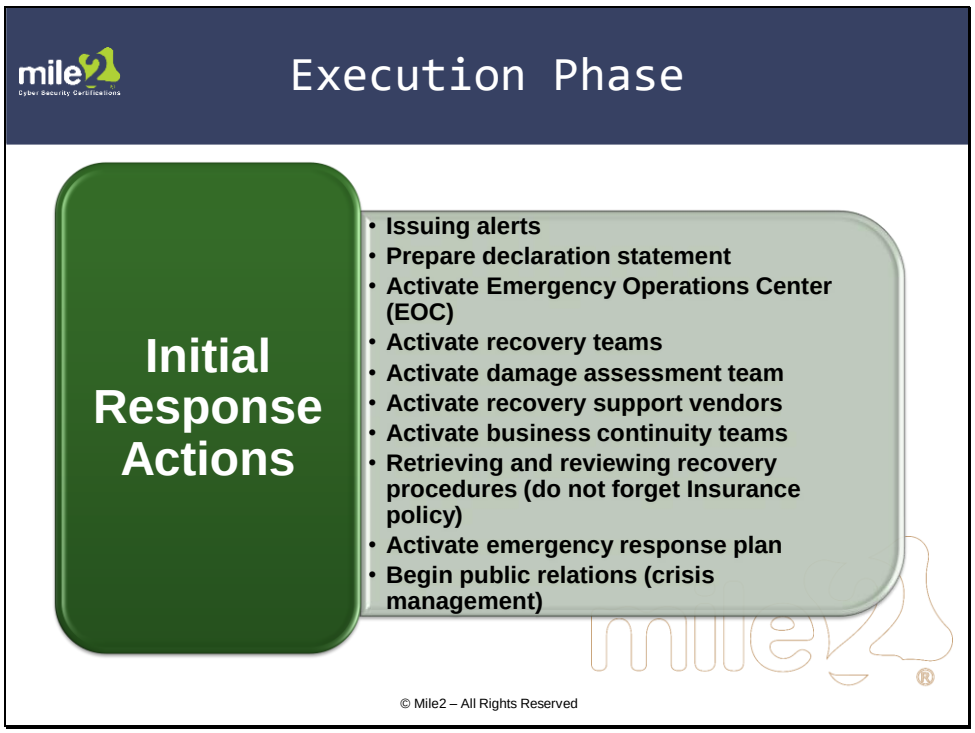
Slide 28


Executing the Plan
Remember the fundamental recovery timing consideration:
• LEAP FORWARD
• No need to accredit the systems at the DR site but do certify that nothing has changed.
• CRAWL BACK
• To the primary site with the least mission critical systems to be used as a validation of the primary site readiness.
• Accreditation is needed!
© Mile2 – All Rights Reserved

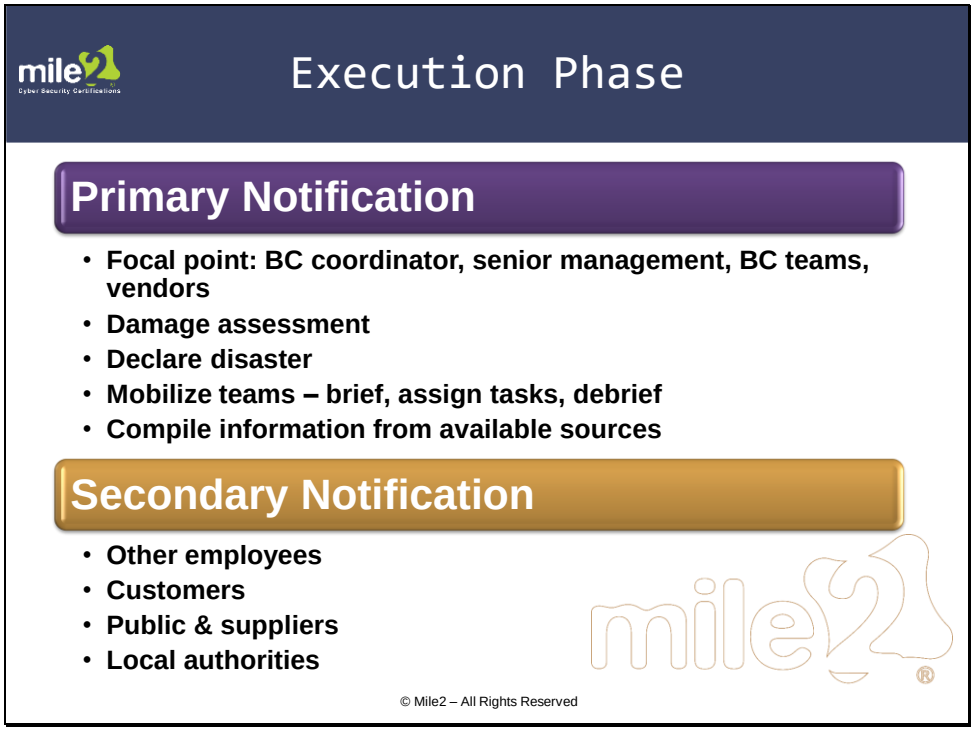
Slide 29


Execution Phase
Escalation Procedure
• Problem Identification
• Define categories of potential problems
• Describe when and how a problem will be escalated and to whom
• Disaster Declaration Criteria
• Determine when a problem becomes a disaster
• Identify who is authorized to declare a disaster
• Contact list (call tree)
• Identify who will be called
• Identify who will make the calls
• List names and contact numbers
• Initial response actions
© Mile2 – All Rights Reserved

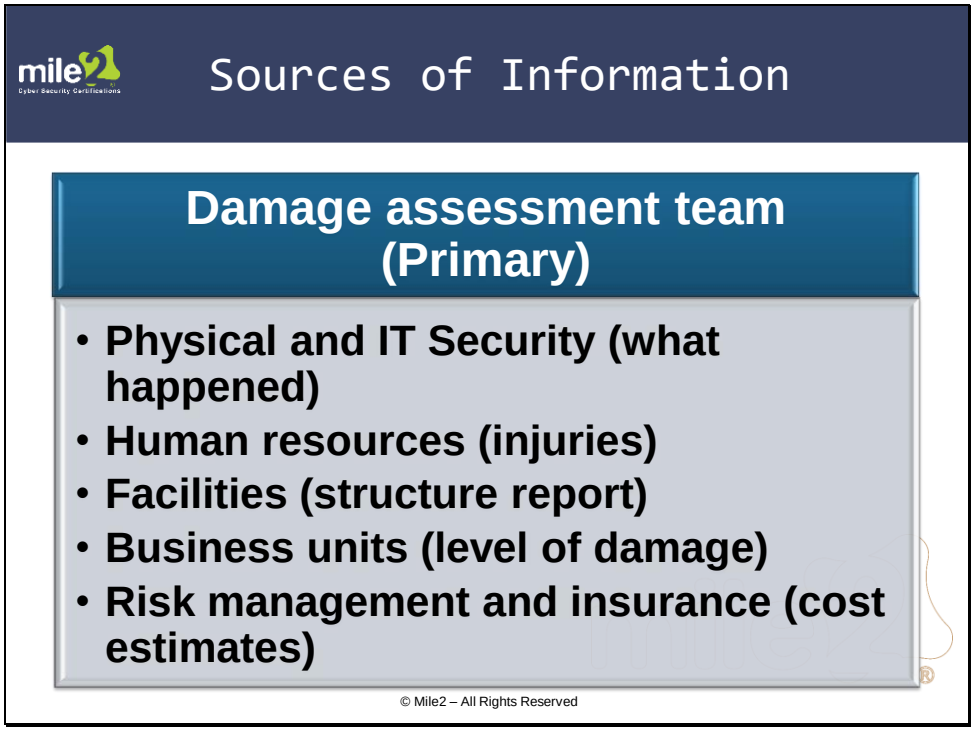
Slide 30


Execution Phase
Initial Response Actions
• Issuing alerts
• Prepare declaration statement
• Activate Emergency Operations Center (EOC)
• Activate recovery teams
• Activate damage assessment team
• Activate recovery support vendors
• Activate business continuity teams
• Retrieving and reviewing recovery procedures (do not forget Insurance policy)
• Activate emergency response plan
• Begin public relations (crisis management)
© Mile2 – All Rights Reserved

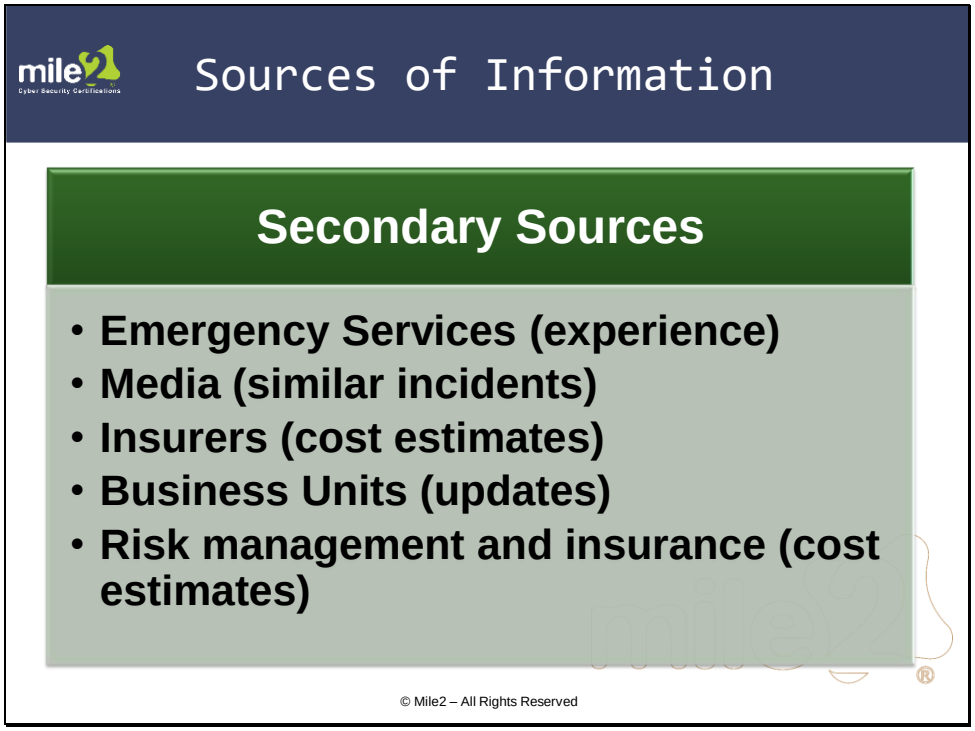
Slide 31


Execution Phase
Primary Notification
• Focal point: BC coordinator, senior management, BC teams, vendors
• Damage assessment
• Declare disaster
• Mobilize teams – brief, assign tasks, debrief
• Compile information from available sources
Secondary Notification
• Other employees
• Customers
• Public & suppliers
• Local authorities
© Mile2 – All Rights Reserved

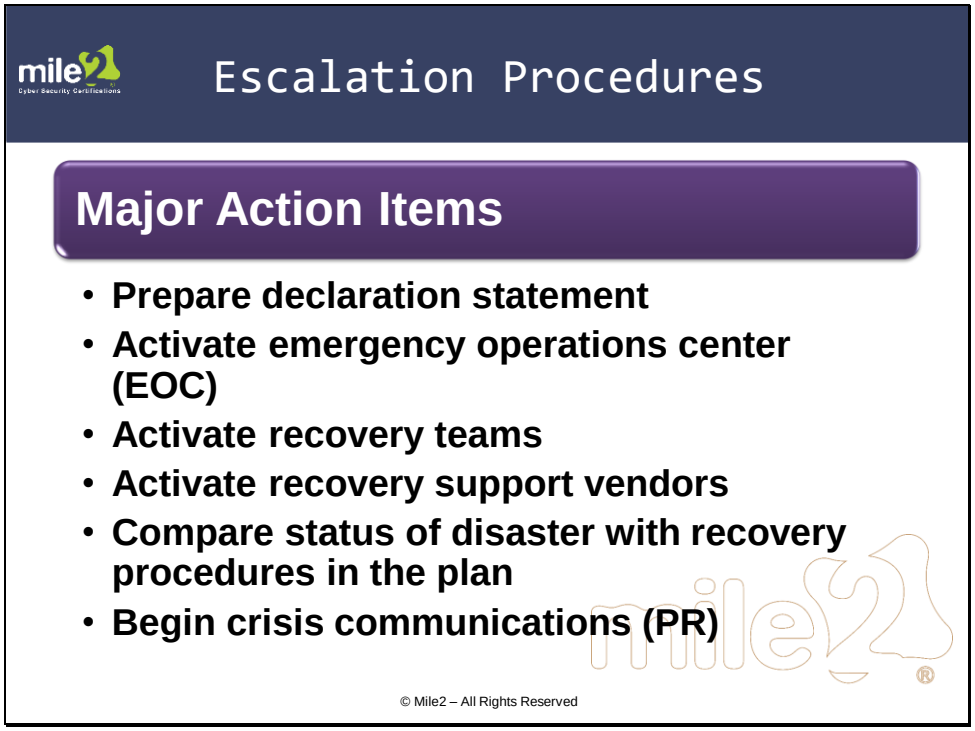
Slide 32


Sources of Information
Damage assessment team (Primary)
• Physical and IT Security (what happened)
• Human resources (injuries)
• Facilities (structure report)
• Business units (level of damage)
• Risk management and insurance (cost estimates)
© Mile2 – All Rights Reserved

Slide 33


Sources of Information
Secondary Sources
• Emergency Services (experience)
• Media (similar incidents)
• Insurers (cost estimates)
• Business Units (updates)
• Risk management and insurance (cost estimates)
© Mile2 – All Rights Reserved

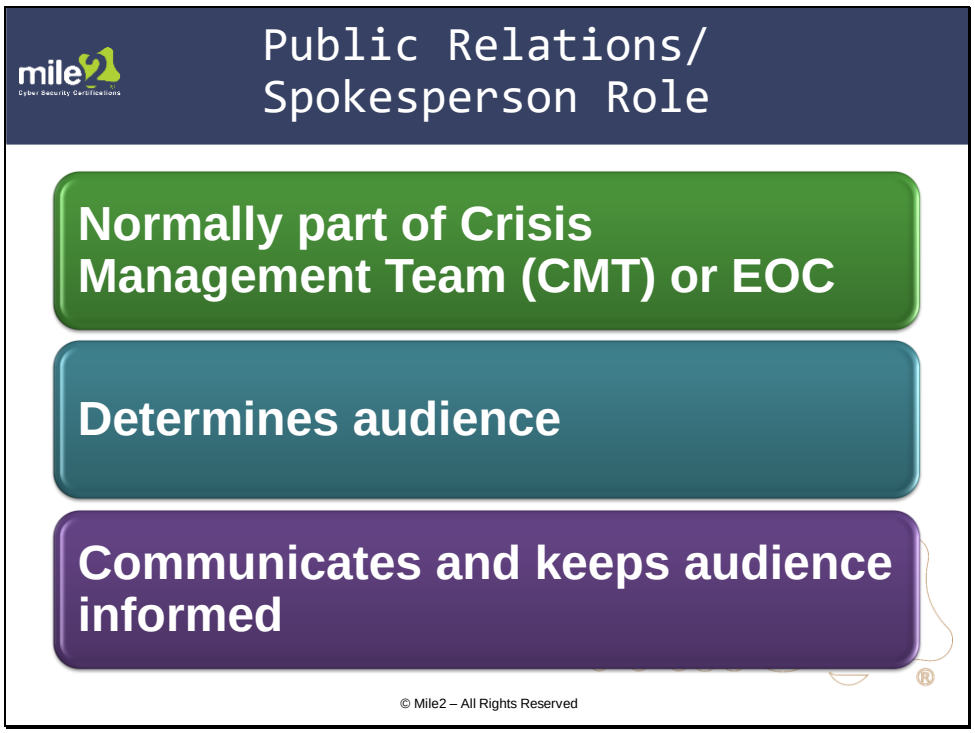
Slide 34


Escalation Procedures
Major Action Items
• Prepare declaration statement
• Activate emergency operations center (EOC)
• Activate recovery teams
• Activate recovery support vendors
• Compare status of disaster with recovery procedures in the plan
• Begin crisis communications (PR)
© Mile2 – All Rights Reserved

Slide 35

Disaster
Declaration Procedures
Activate Public Relations Coordination – Plan
• Use pre-arranged PR program or delegate to an expert / firm
• Update prepared press releases
• Develop schedule for press conferences and interviews
• Communicate name of spokesperson
• Prepare to address all of the necessary audiences
© Mile2 – All Rights Reserved

Slide 36


Public Relations/
Spokesperson Role
Normally part of Crisis Management Team (CMT) or EOC
Determines audience
Communicates and keeps audience informed
© Mile2 – All Rights Reserved

Slide 37

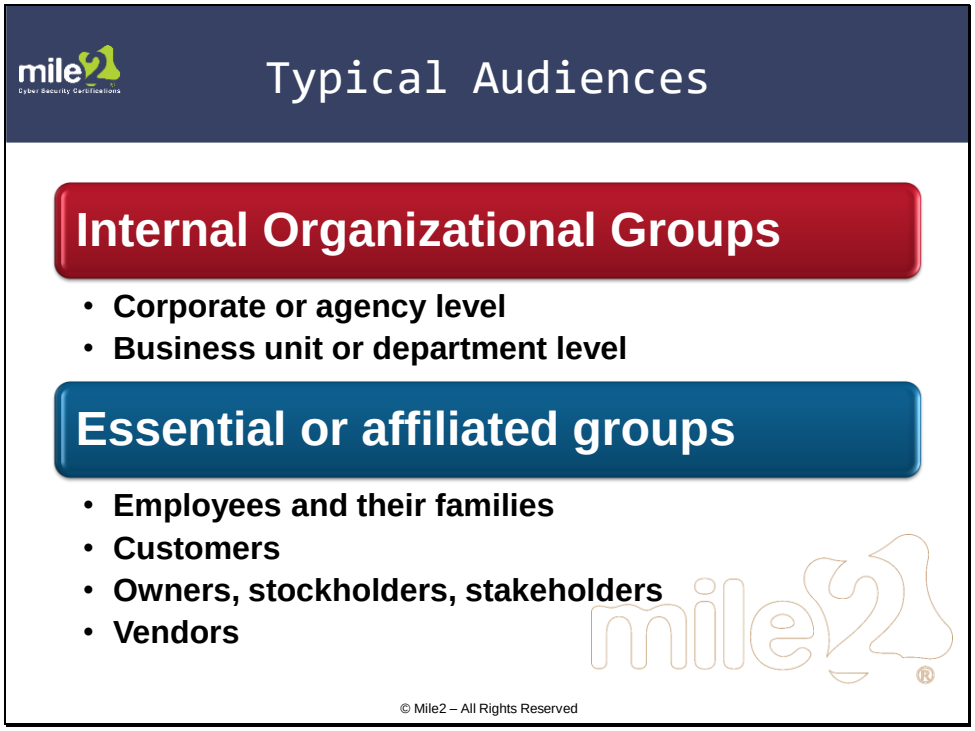
# Typical Audiences

## External

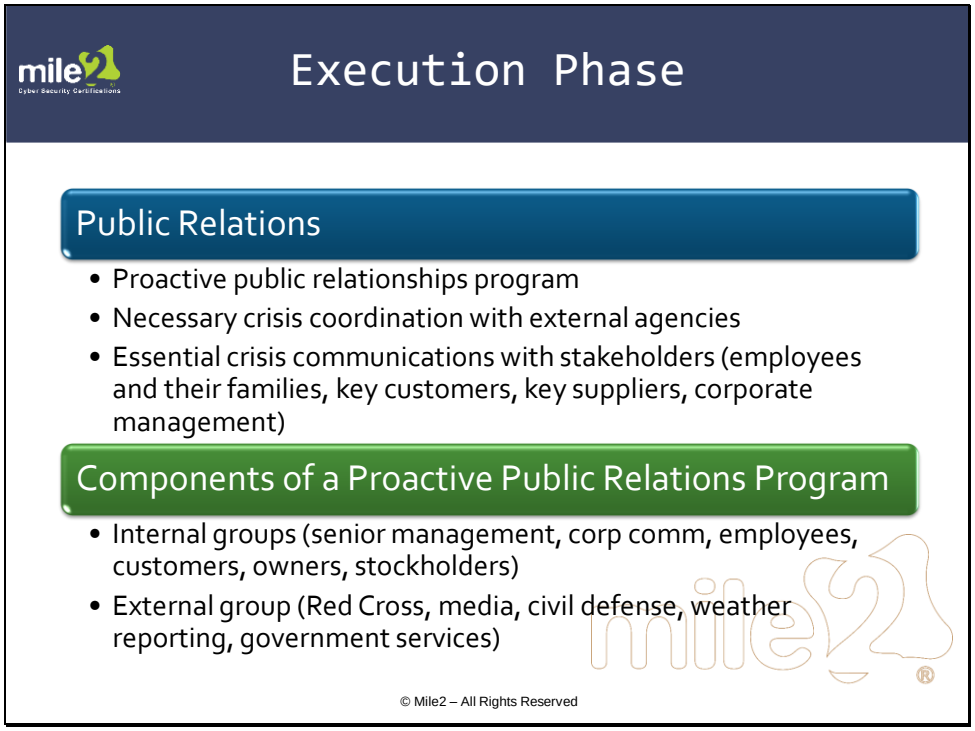
- Media
  - Newspapers, radio, TV, internet sites, social media
- Public
- Local, State, and Federal Emergency services, civil defense, etc.
- Government Agencies
  - State and local fire authorities, law enforcement, Emergency Medical Services (EMS), and transportation

© Mile2 – All Rights Reserved

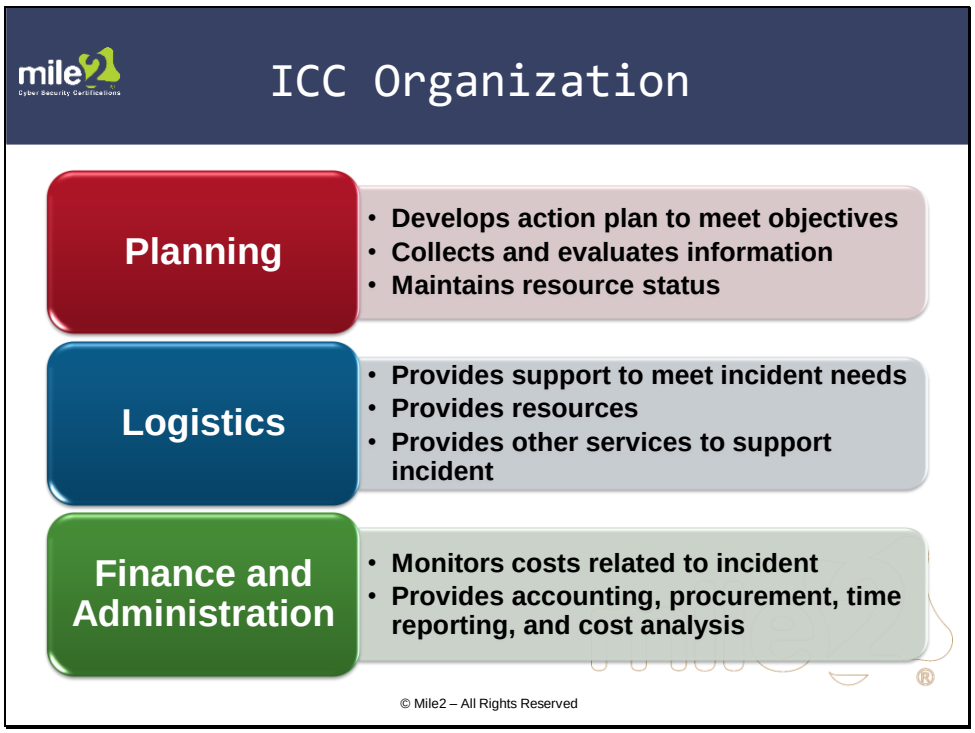
Slide 38


Typical Audiences
Internal Organizational Groups
• Corporate or agency level
• Business unit or department level
Essential or affiliated groups
• Employees and their families
• Customers
• Owners, stockholders, stakeholders
• Vendors
© Mile2 – All Rights Reserved

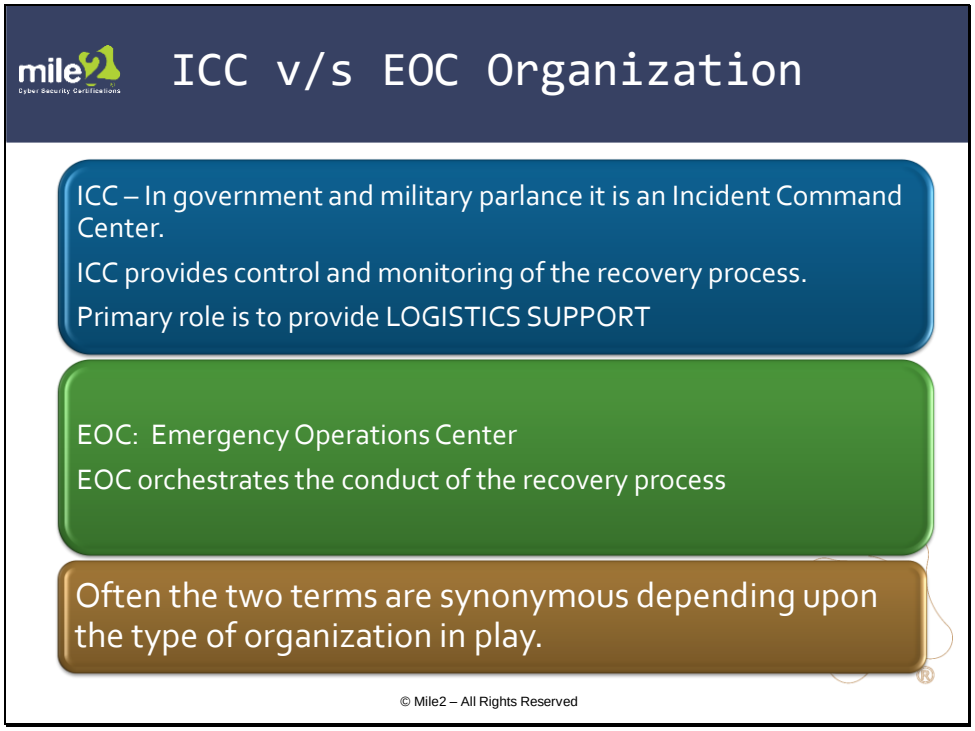
Slide 39


Execution Phase
Public Relations
• Proactive public relationships program
• Necessary crisis coordination with external agencies
• Essential crisis communications with stakeholders (employees and their families, key customers, key suppliers, corporate management)
Components of a Proactive Public Relations Program
• Internal groups (senior management, corp comm, employees, customers, owners, stockholders)
• External group (Red Cross, media, civil defense, weather reporting, government services)
© Mile2 – All Rights Reserved

Slide 40


ICC Organization
Planning
• Develops action plan to meet objectives
• Collects and evaluates information
• Maintains resource status
Logistics
• Provides support to meet incident needs
• Provides resources
• Provides other services to support incident
Finance and Administration
• Monitors costs related to incident
• Provides accounting, procurement, time reporting, and cost analysis
© Mile2 – All Rights Reserved

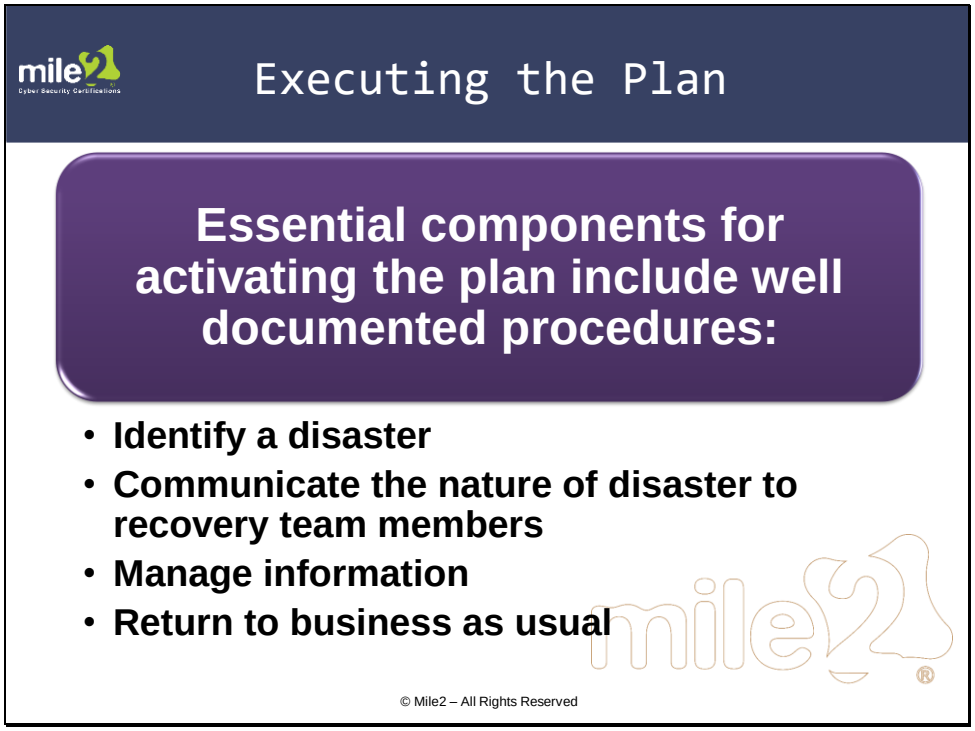
Slide 41


ICC v/s EOC Organization
ICC – In government and military parlance it is an Incident Command Center.
ICC provides control and monitoring of the recovery process.
Primary role is to provide LOGISTICS SUPPORT
EOC: Emergency Operations Center
EOC orchestrates the conduct of the recovery process
Often the two terms are synonymous depending upon the type of organization in play.
© Mile2 – All Rights Reserved

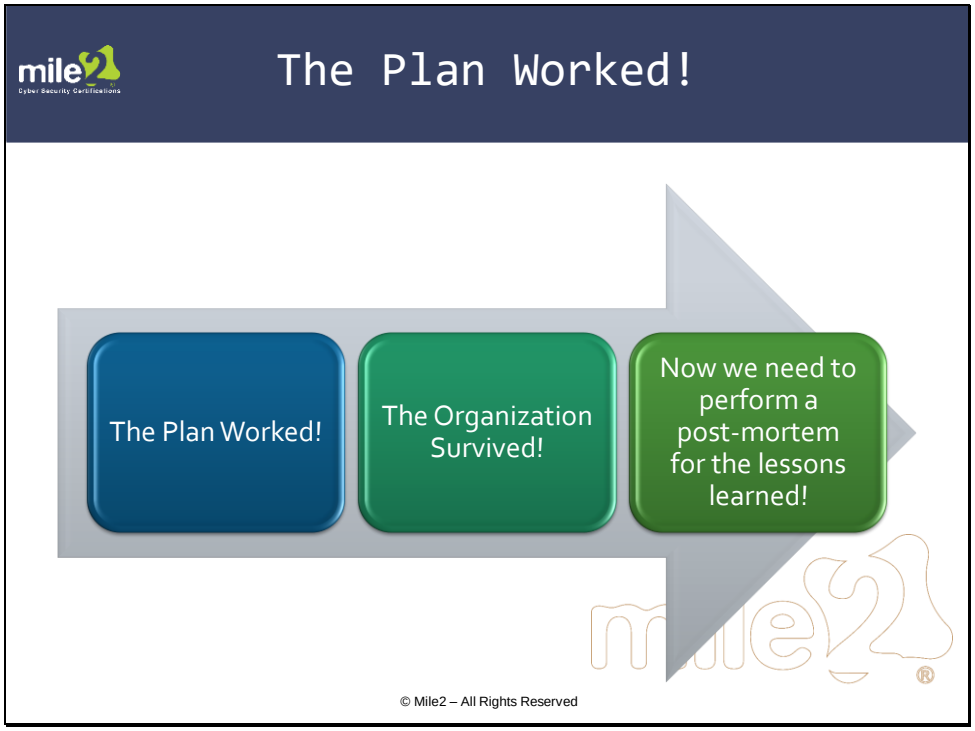
Slide 42

Be Prepared to Work with Public Authorities
Identify sources of information on applicable laws and regulations
Identify applicable regulations and laws concerning environmental issues
Identify statutory industry requirements
Ensure your plans meet all regulatory and statutory requirements
Meet and work with local authorities
© Mile2 – All Rights Reserved

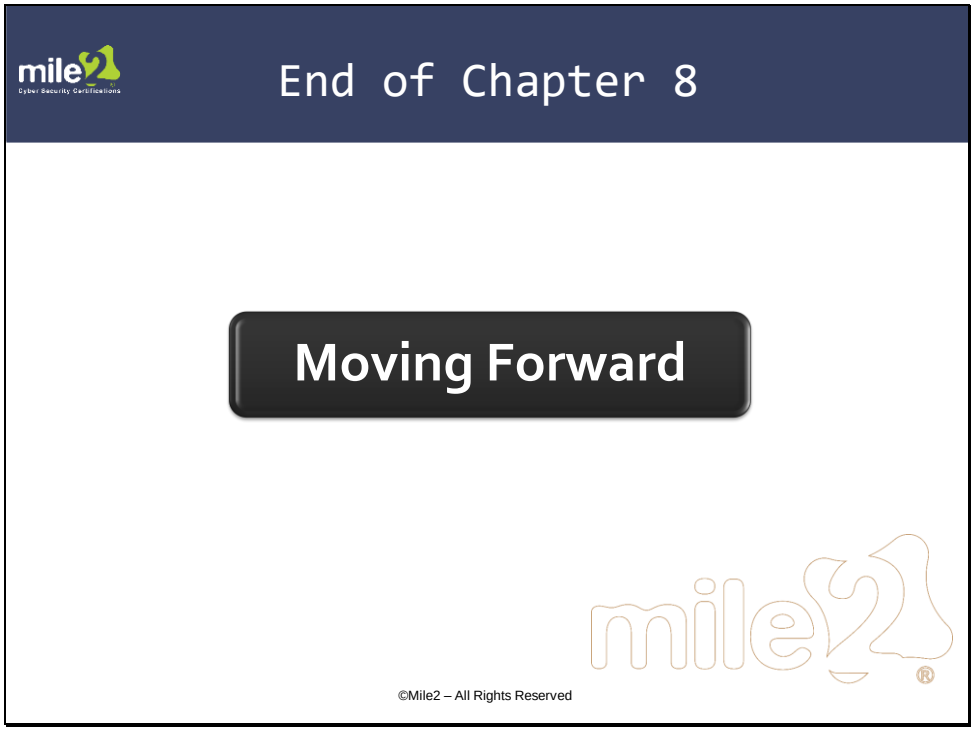
Slide 43


Executing the Plan
Essential components for activating the plan include well documented procedures:
• Identify a disaster
• Communicate the nature of disaster to recovery team members
• Manage information
• Return to business as usual
© Mile2 – All Rights Reserved

Slide 44


The Plan Worked!
The Plan Worked!
The Organization Survived!
Now we need to perform a post-mortem for the lessons learned!
© Mile2 – All Rights Reserved

Slide 45



# Questions and Answers

## Review Questions:

1. If system and application changes occur outside of the Change Control program, the greatest concern is that:
    A. The BCP becomes obsolete
    B. The time for implementation will increase
    C. These changes will be identified after implementation
    D. Version control of the changes will be a challenge to maintain consistency

2. BCP plan maintenance and updates should be done:
    A. Annually
    B. Quarterly
    C. After every change
    D. It depends on what is appropriate for the environment based on the BC Policy

## Answer Key:

1. A
   If system and application changes occur outside of the change control program, the greatest concern is that the BCP becomes obsolete.

2. D
   BCP plan maintenance and updates depend on what is appropriate for the environment based on the BC Policy.