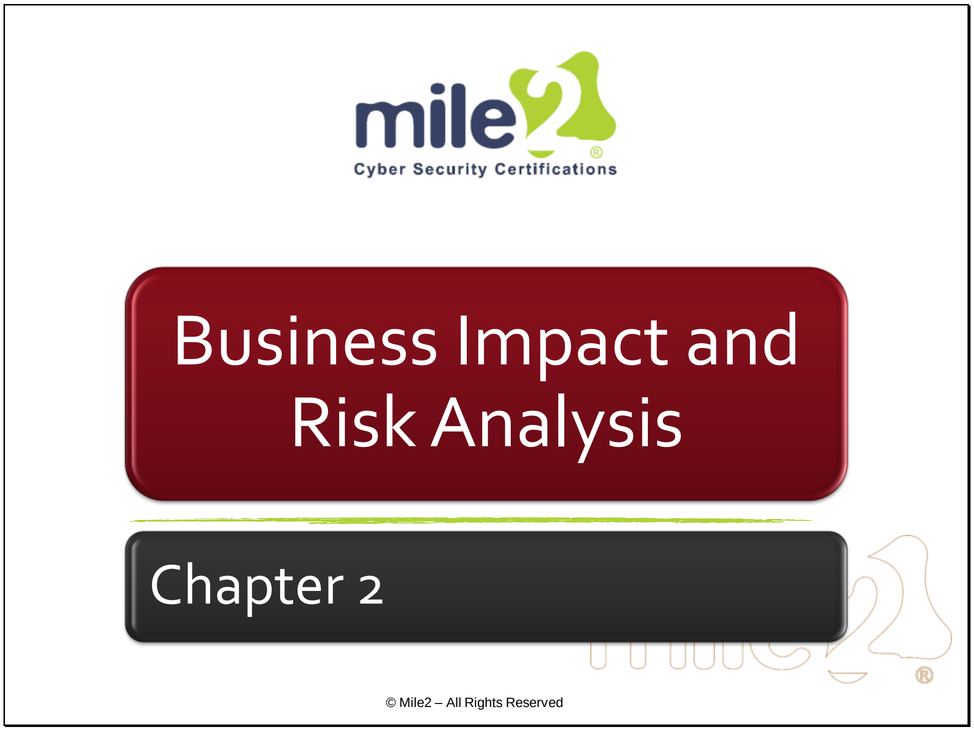
CDRE - Certified Disaster Recovery Engineer

Chapter 2 - Business Impact and Risk Analysis

WORKBOOK

Slide 1

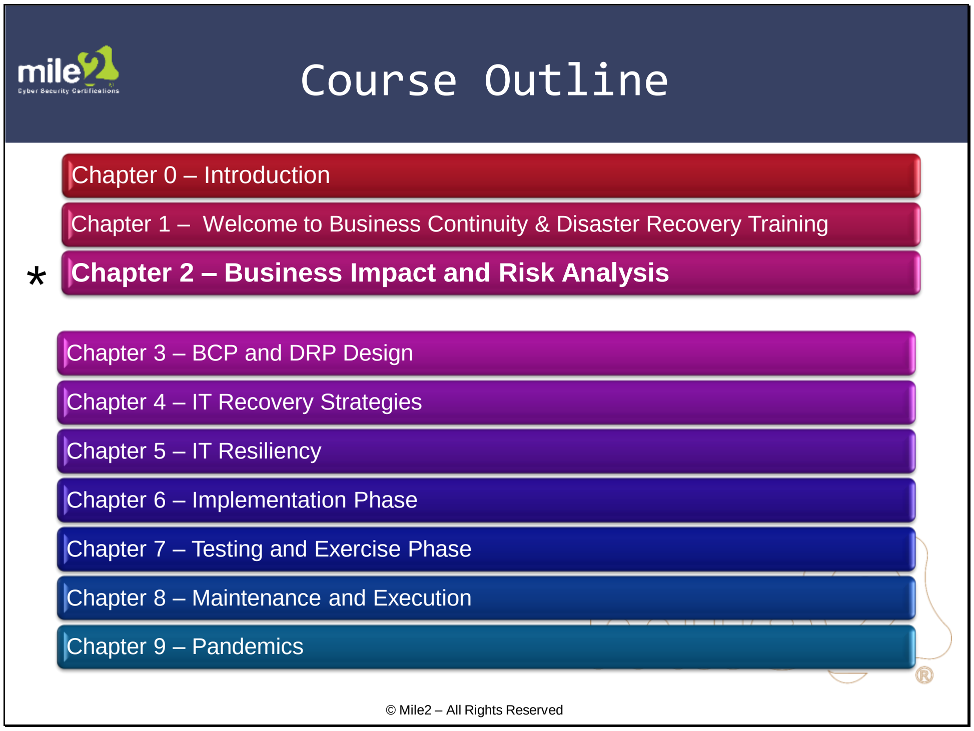


Cyber Security Certifications

Business Impact and Risk Analysis

Chapter 2

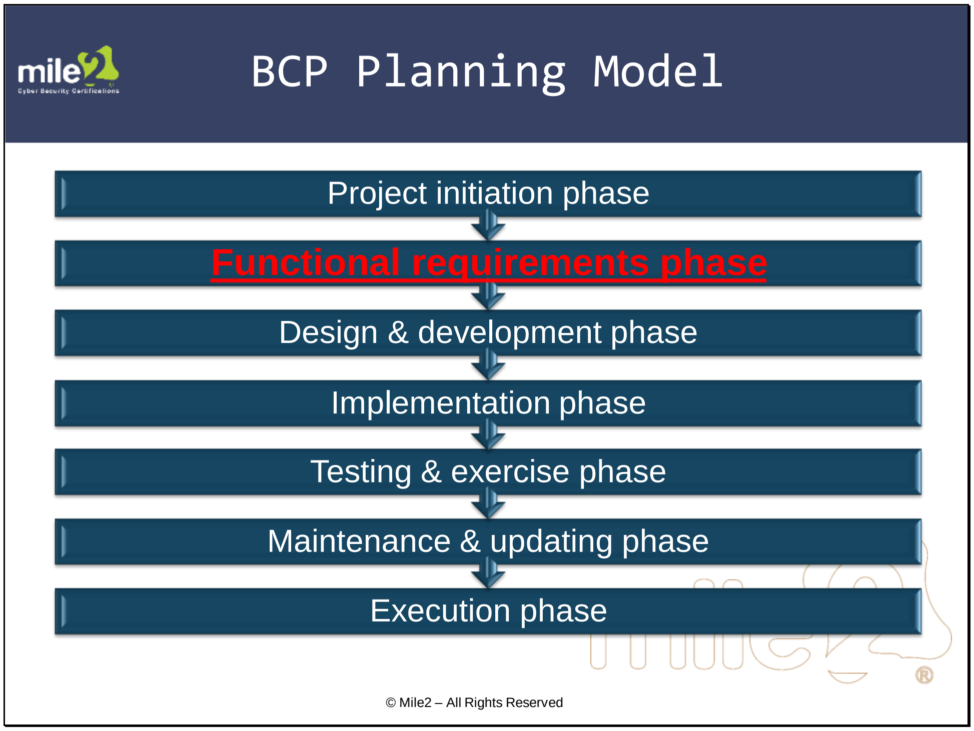
Slide 2



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

Slide 3



BCP Planning Model

Project initiation phase

Functional requirements phase

Design & development phase

Implementation phase

Testing & exercise phase

Maintenance & updating phase

Execution phase

____

____

____

____

____

____

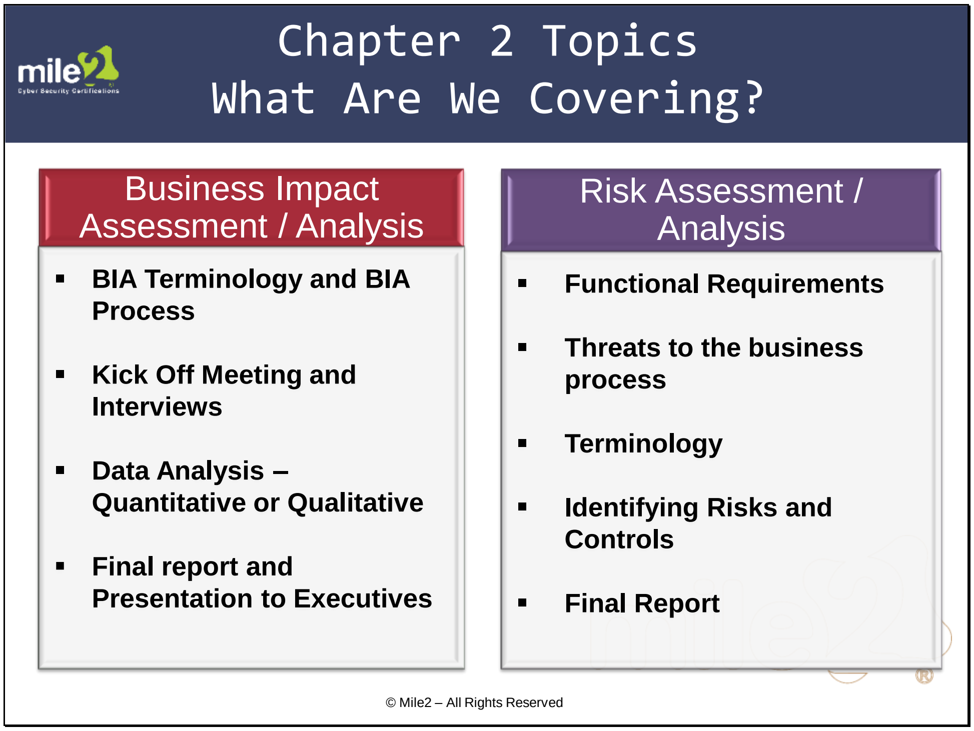
____

____

____

____

Slide 4



Chapter 2 Topics
What Are We Covering?

Business Impact Assessment / Analysis

- BIA Terminology and BIA Process
- Kick Off Meeting and Interviews
- Data Analysis – Quantitative or Qualitative
- Final report and Presentation to Executives

Risk Assessment / Analysis

- Functional Requirements
- Threats to the business process
- Terminology
- Identifying Risks and Controls
- Final Report

Slide 5

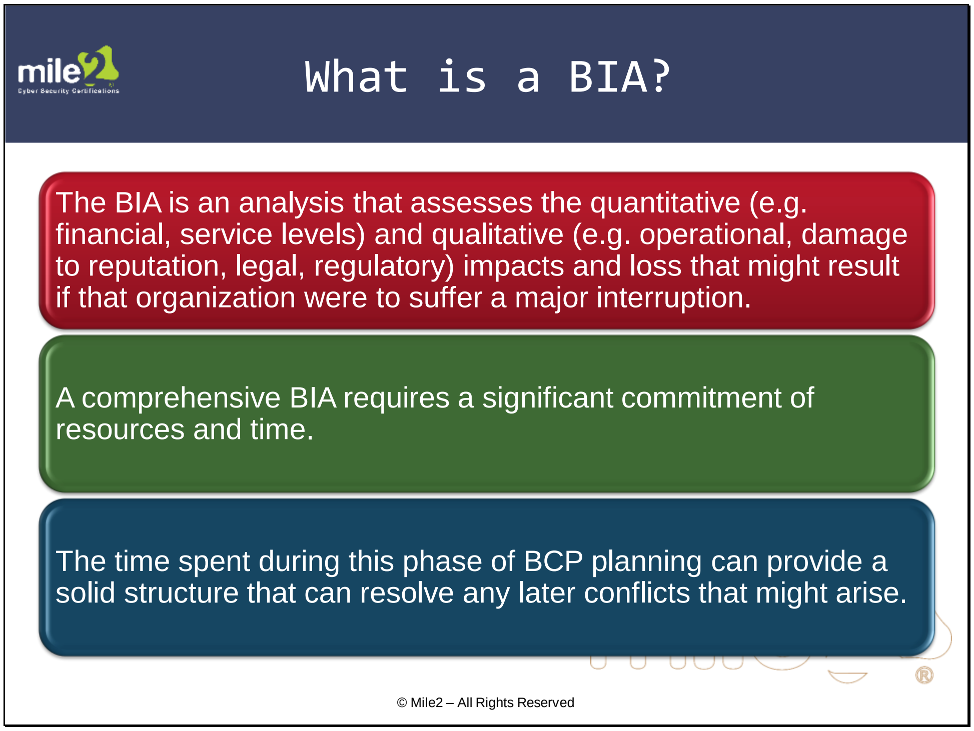
mile2

Cyber Security Certifications

BCP
Planning Phase –
Functional Requirement Phase

Section 1

Slide 6



What is a BIA?

The BIA is an analysis that assesses the quantitative (e.g. financial, service levels) and qualitative (e.g. operational, damage to reputation, legal, regulatory) impacts and loss that might result if that organization were to suffer a major interruption.

A comprehensive BIA requires a significant commitment of resources and time.

The time spent during this phase of BCP planning can provide a solid structure that can resolve any later conflicts that might arise.

____

____

____

____

____

____

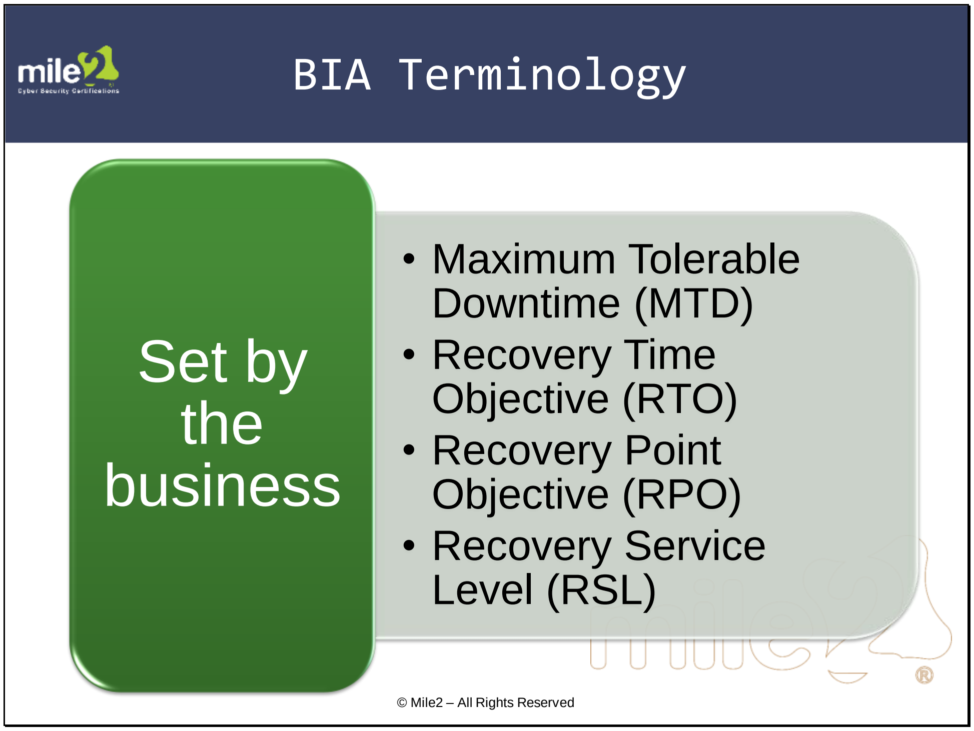
____

____

____

____

Slide 7

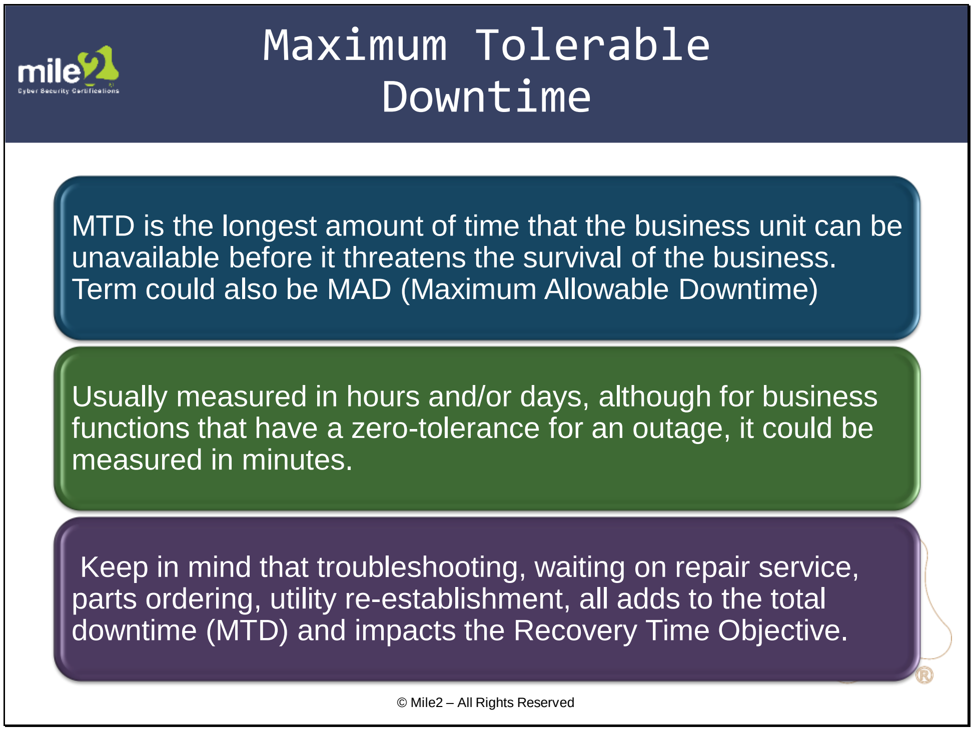


BIA Terminology

Set by the business

- Maximum Tolerable Downtime (MTD)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Recovery Service Level (RSL)

Slide 8



Maximum Tolerable Downtime

MTD is the longest amount of time that the business unit can be unavailable before it threatens the survival of the business. Term could also be MAD (Maximum Allowable Downtime)

Usually measured in hours and/or days, although for business functions that have a zero-tolerance for an outage, it could be measured in minutes.

Keep in mind that troubleshooting, waiting on repair service, parts ordering, utility re-establishment, all adds to the total downtime (MTD) and impacts the Recovery Time Objective.

____

____

____

____

____

____

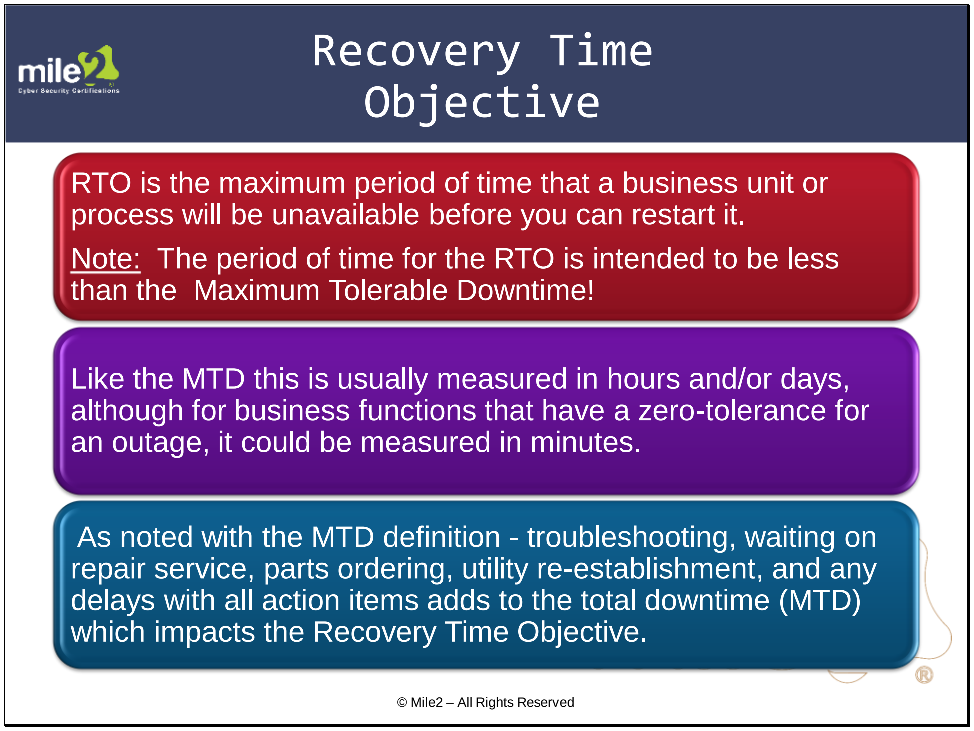
____

____

____

____

Slide 9



Recovery Time Objective

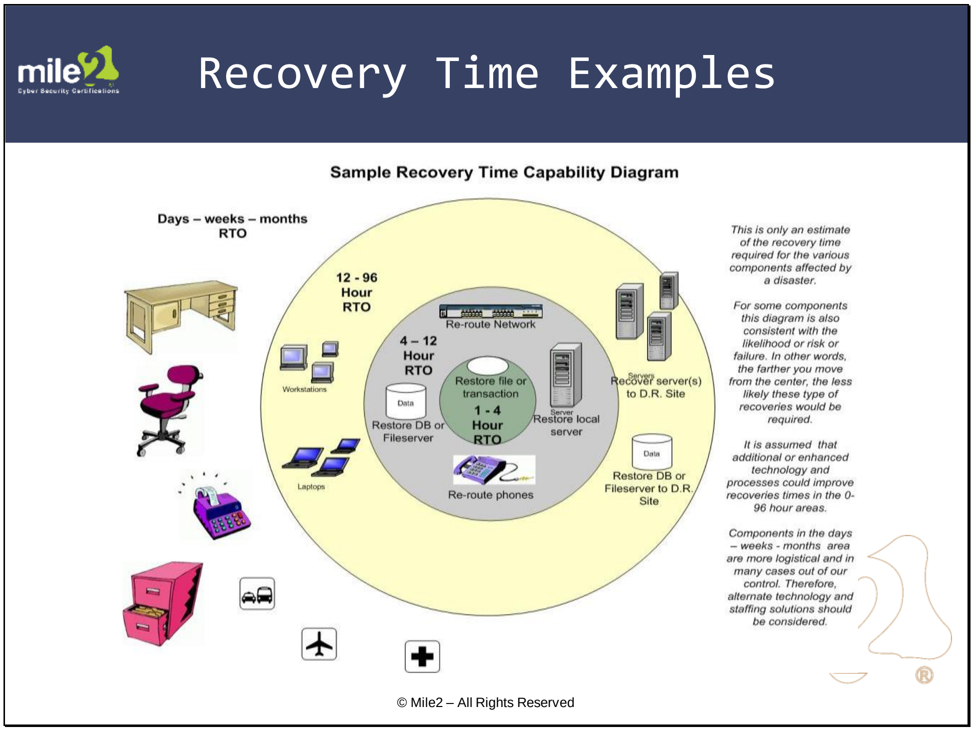
RTO is the maximum period of time that a business unit or process will be unavailable before you can restart it.

Note: The period of time for the RTO is intended to be less than the Maximum Tolerable Downtime!

Like the MTD this is usually measured in hours and/or days, although for business functions that have a zero-tolerance for an outage, it could be measured in minutes.

As noted with the MTD definition - troubleshooting, waiting on repair service, parts ordering, utility re-establishment, and any delays with all action items adds to the total downtime (MTD) which impacts the Recovery Time Objective.

Slide 10



Recovery Time Examples

This is only an estimate of the recovery time required for the various components affected by a disaster.

For some components this diagram is also consistent with the likelihood or risk or failure. In other words, the farther you move from the center, the less likely these type of recoveries would be required.

It is assumed that additional or enhanced technology and processes could improve recoveries times in the 0-96 hour areas.

Components in the days – weeks - months area are more logistical and in many cases out of our control. Therefore, alternate technology and staffing solutions should be considered.

____

____

____

____

____

____

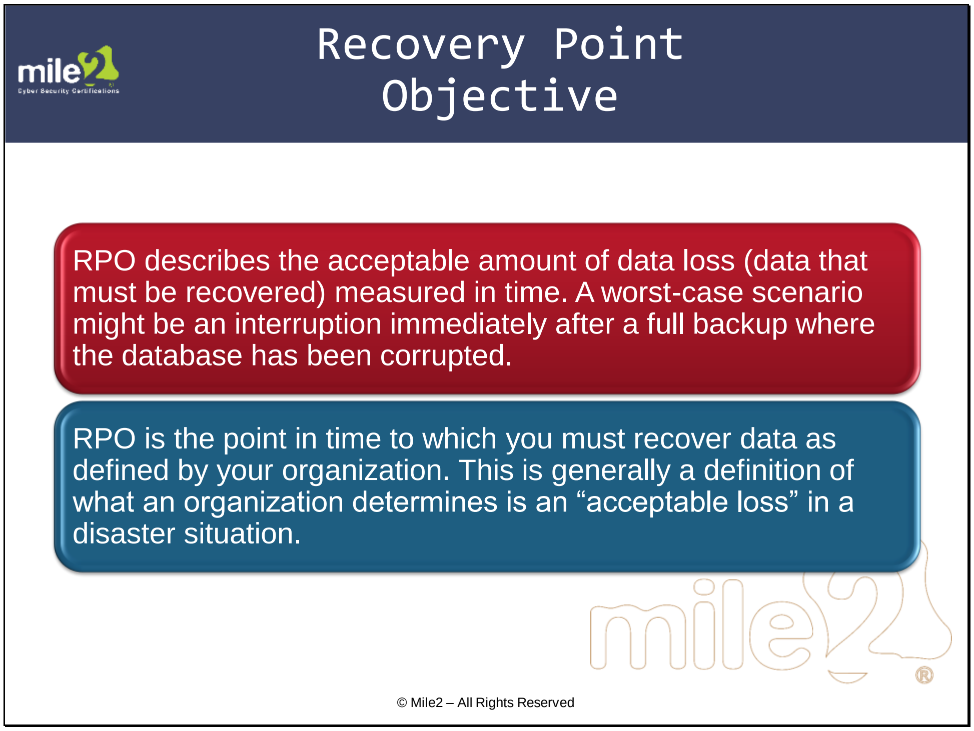
____

____

____

____

Slide 11

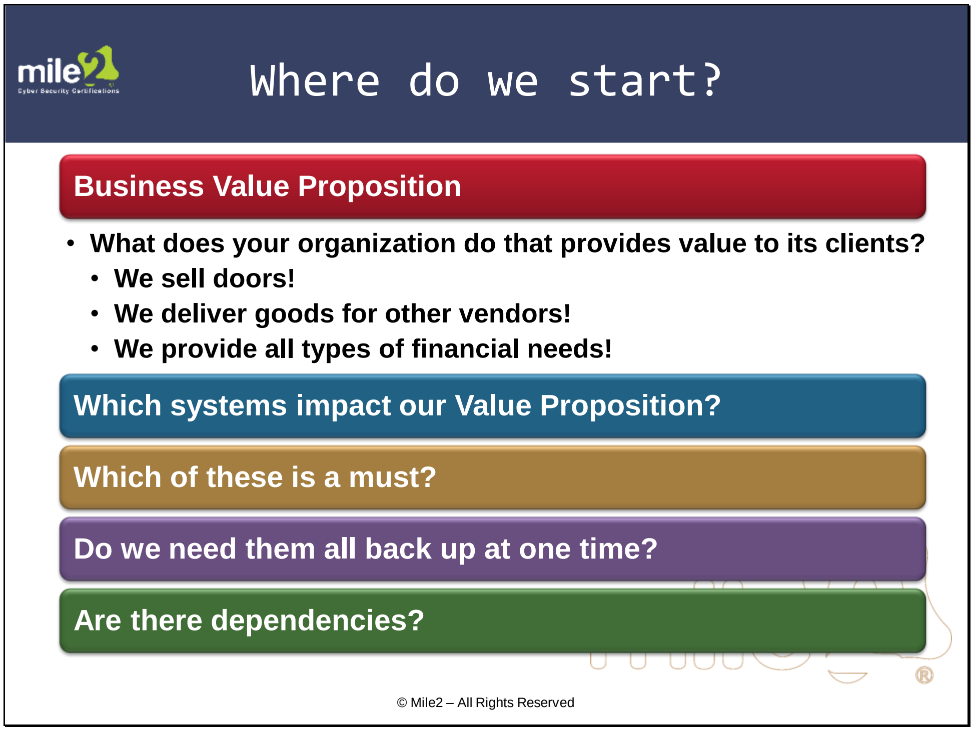


Recovery Point Objective

RPO describes the acceptable amount of data loss (data that must be recovered) measured in time. A worst-case scenario might be an interruption immediately after a full backup where the database has been corrupted.

RPO is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an “acceptable loss” in a disaster situation.

Slide 12



Where do we start?

Business Value Proposition

- **What does your organization do that provides value to its clients?**
  - **We sell doors!**
  - **We deliver goods for other vendors!**
  - **We provide all types of financial needs!**

Which systems impact our Value Proposition?

Which of these is a must?

Do we need them all back up at one time?

Are there dependencies?

____

____

____

____

____

____

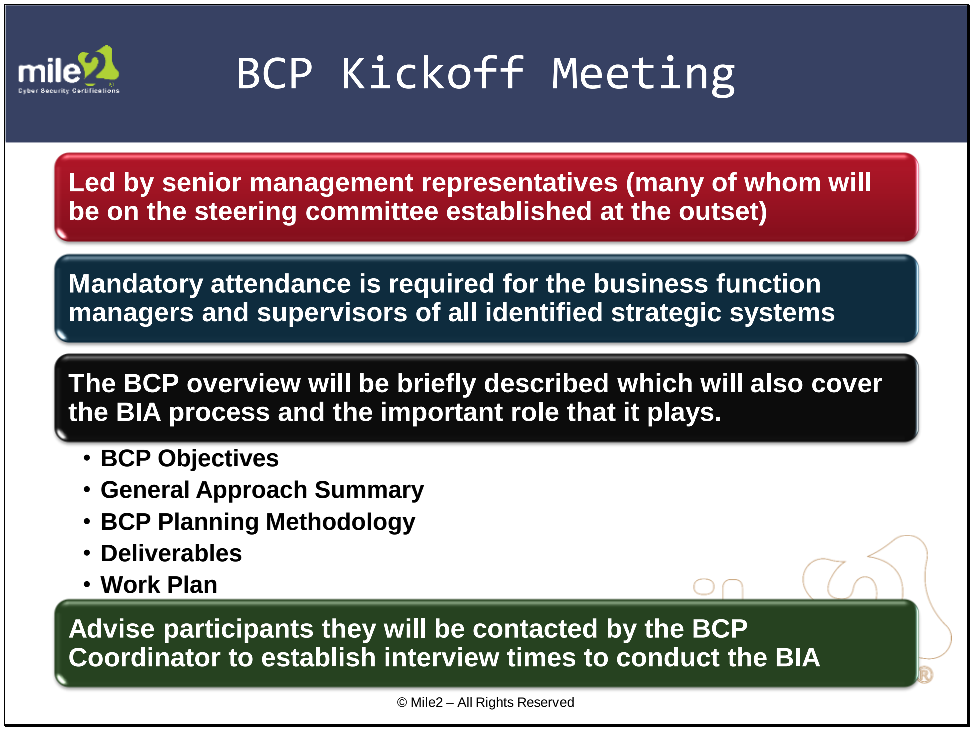
____

____

____

____

Slide 13



BCP Kickoff Meeting

Led by senior management representatives (many of whom will be on the steering committee established at the outset)

Mandatory attendance is required for the business function managers and supervisors of all identified strategic systems

The BCP overview will be briefly described which will also cover the BIA process and the important role that it plays.

- BCP Objectives
- General Approach Summary
- BCP Planning Methodology
- Deliverables
- Work Plan

Advise participants they will be contacted by the BCP Coordinator to establish interview times to conduct the BIA

____

____

____

____

____

____

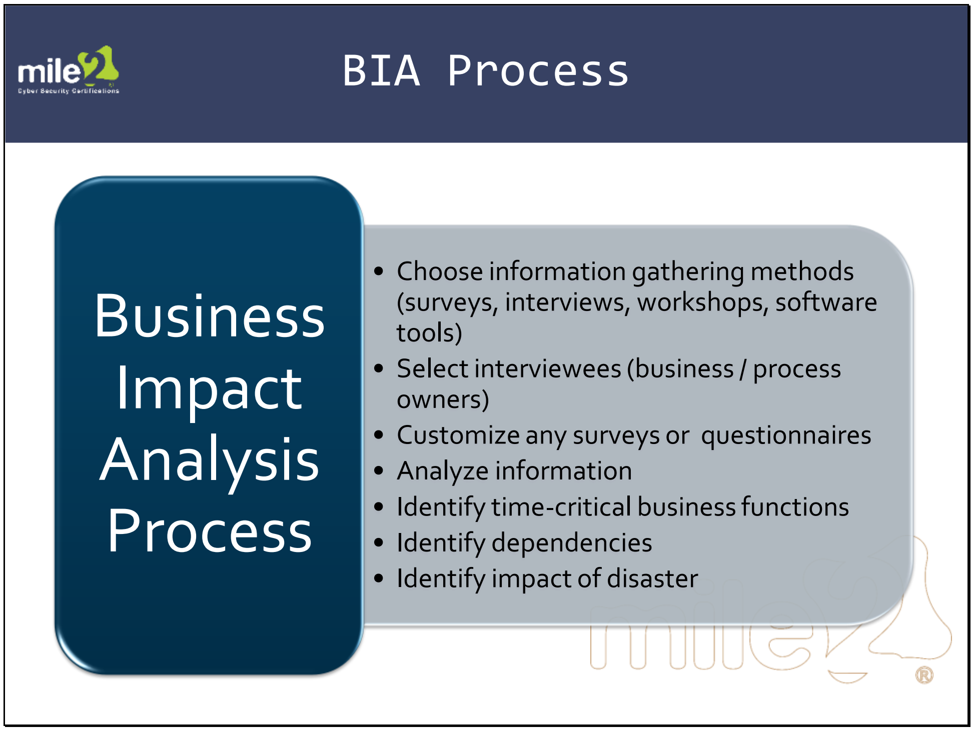
____

____

____

____

Slide 14



BIA Process

Business Impact Analysis Process

- Choose information gathering methods (surveys, interviews, workshops, software tools)
- Select interviewees (business / process owners)
- Customize any surveys or questionnaires
- Analyze information
- Identify time-critical business functions
- Identify dependencies
- Identify impact of disaster

____

____

____

____

____

____

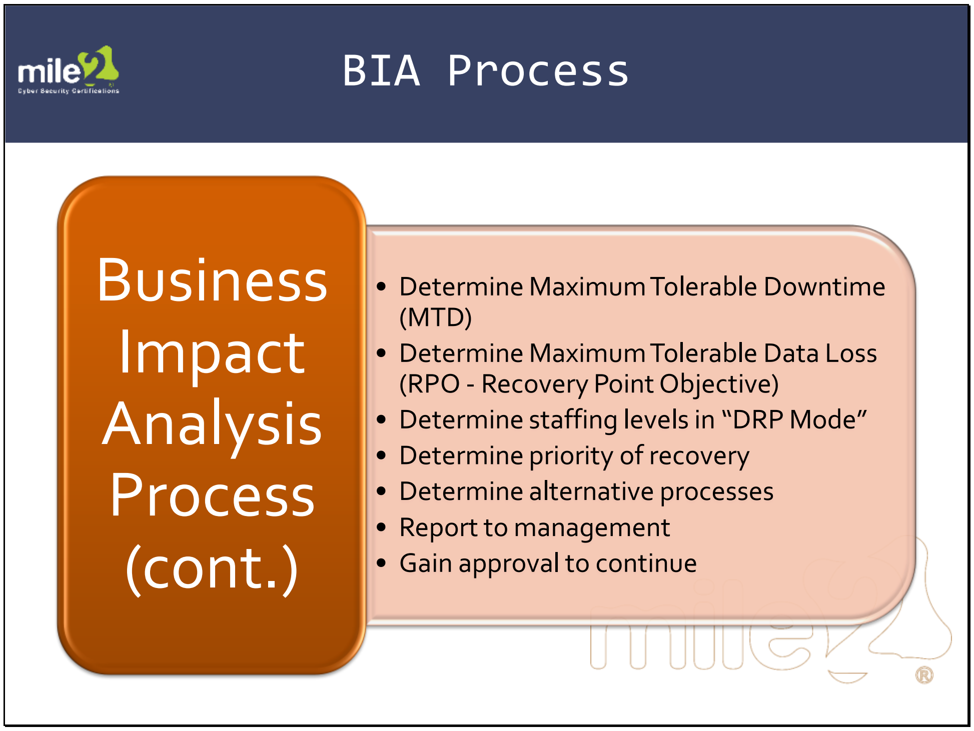
____

____

____

____

Slide 15

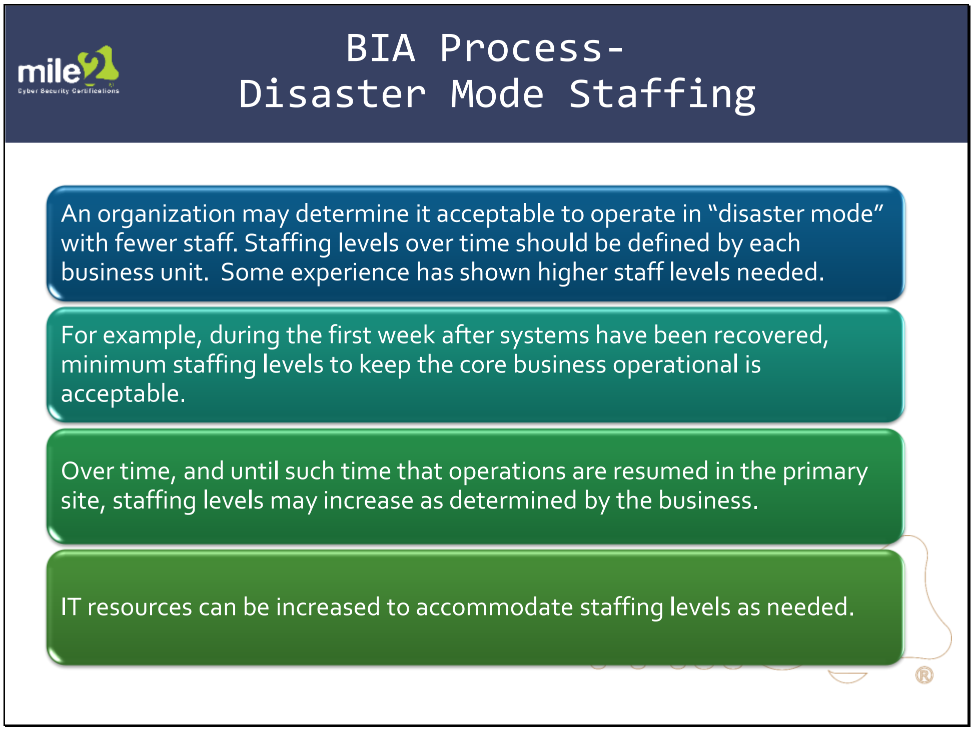


BIA Process

Business Impact Analysis Process (cont.)

- Determine Maximum Tolerable Downtime (MTD)
- Determine Maximum Tolerable Data Loss (RPO - Recovery Point Objective)
- Determine staffing levels in "DRP Mode"
- Determine priority of recovery
- Determine alternative processes
- Report to management
- Gain approval to continue

Slide 16



BIA Process- Disaster Mode Staffing

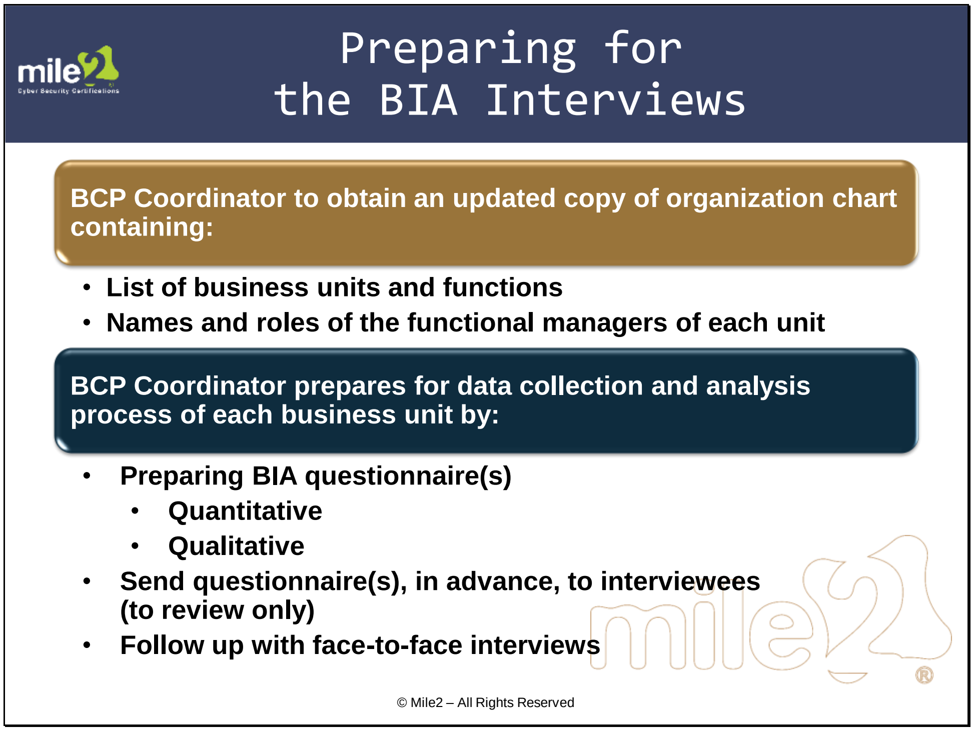
An organization may determine it acceptable to operate in “disaster mode” with fewer staff. Staffing levels over time should be defined by each business unit. Some experience has shown higher staff levels needed.

For example, during the first week after systems have been recovered, minimum staffing levels to keep the core business operational is acceptable.

Over time, and until such time that operations are resumed in the primary site, staffing levels may increase as determined by the business.

IT resources can be increased to accommodate staffing levels as needed.

Slide 17



Preparing for the BIA Interviews

BCP Coordinator to obtain an updated copy of organization chart containing:

- List of business units and functions
- Names and roles of the functional managers of each unit

BCP Coordinator prepares for data collection and analysis process of each business unit by:

- Preparing BIA questionnaire(s)
  - Quantitative
  - Qualitative
- Send questionnaire(s), in advance, to interviewees (to review only)
- Follow up with face-to-face interviews

____

____

____

____

____

____

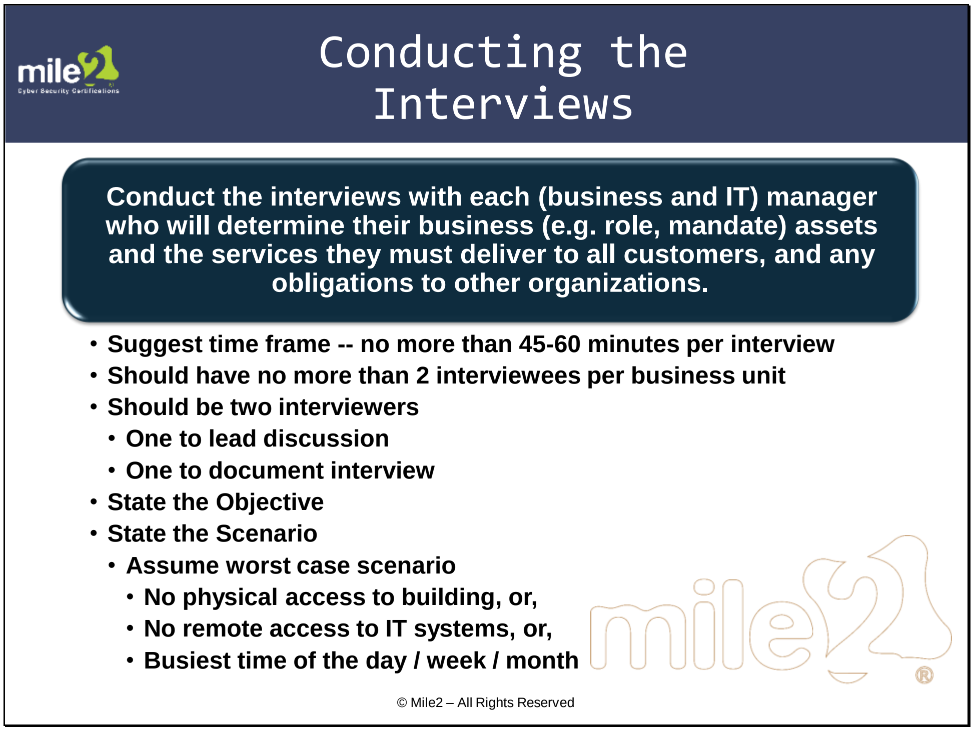
____

____

____

____

Slide 18

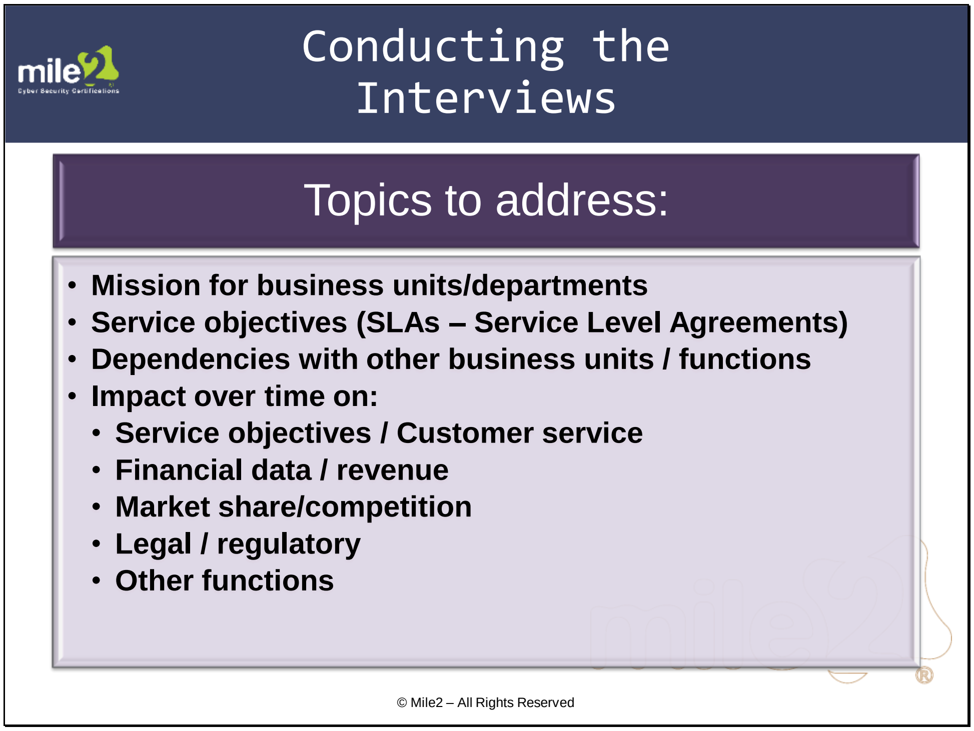


Conducting the Interviews

Conduct the interviews with each (business and IT) manager who will determine their business (e.g. role, mandate) assets and the services they must deliver to all customers, and any obligations to other organizations.

- **Suggest time frame -- no more than 45-60 minutes per interview**
- **Should have no more than 2 interviewees per business unit**
- **Should be two interviewers**
  - **One to lead discussion**
  - **One to document interview**
- **State the Objective**
- **State the Scenario**
  - **Assume worst case scenario**
    - **No physical access to building, or,**
    - **No remote access to IT systems, or,**
    - **Busiest time of the day / week / month**

Slide 19

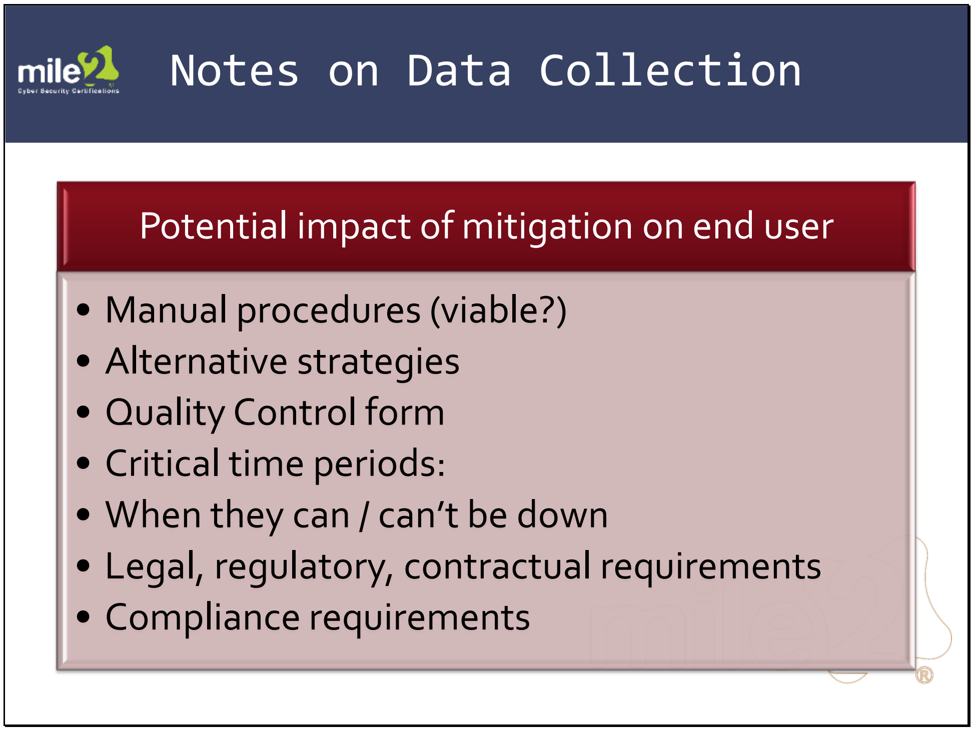


Conducting the Interviews

Topics to address:

- Mission for business units/departments
- Service objectives (SLAs – Service Level Agreements)
- Dependencies with other business units / functions
- Impact over time on:
  - Service objectives / Customer service
  - Financial data / revenue
  - Market share/competition
  - Legal / regulatory
  - Other functions

Slide 20

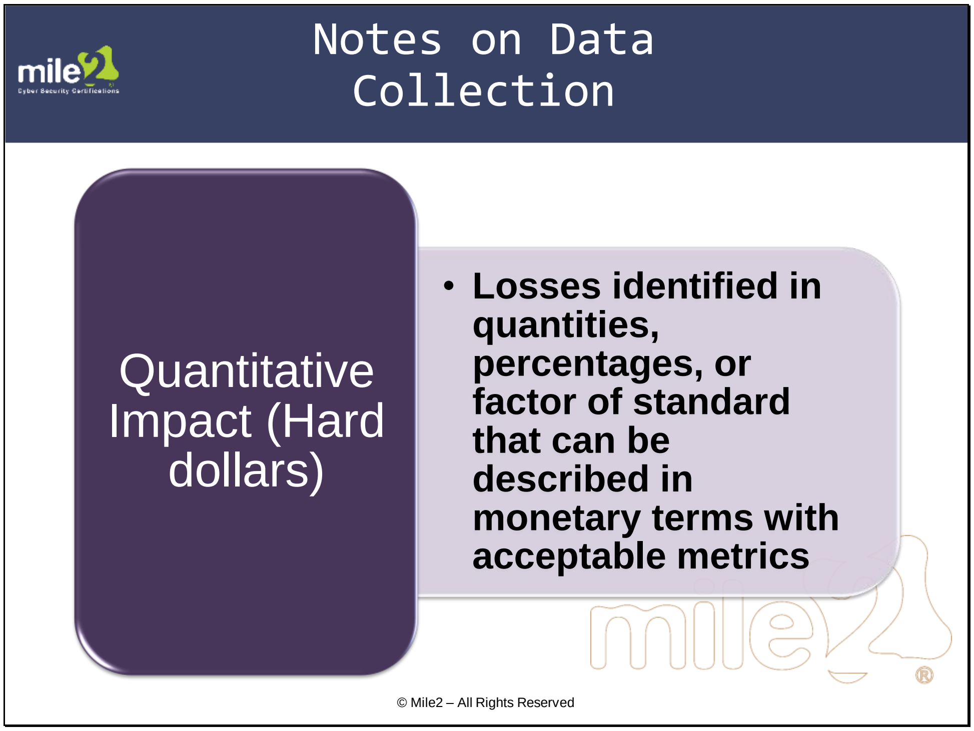


Notes on Data Collection

Potential impact of mitigation on end user

- Manual procedures (viable?)
- Alternative strategies
- Quality Control form
- Critical time periods:
- When they can / can’t be down
- Legal, regulatory, contractual requirements
- Compliance requirements

Slide 21

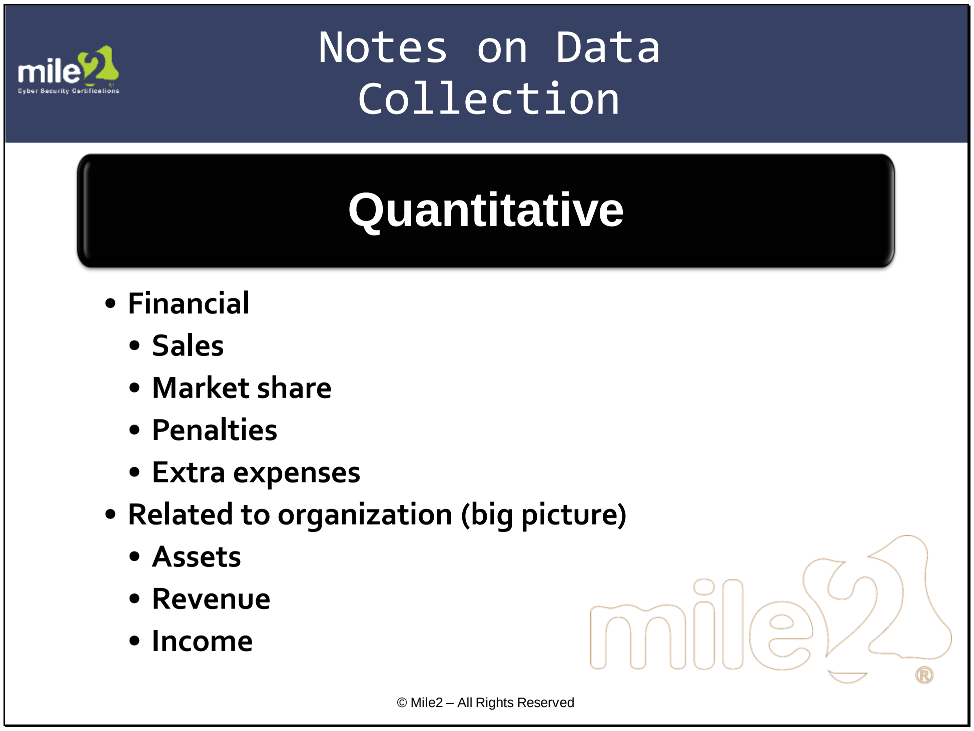


Notes on Data Collection

Quantitative Impact (Hard dollars)

- Losses identified in quantities, percentages, or factor of standard that can be described in monetary terms with acceptable metrics

Slide 22



Notes on Data Collection

Quantitative

- Financial
  - Sales
  - Market share
  - Penalties
  - Extra expenses
- Related to organization (big picture)
  - Assets
  - Revenue
  - Income

____

____

____

____

____

____

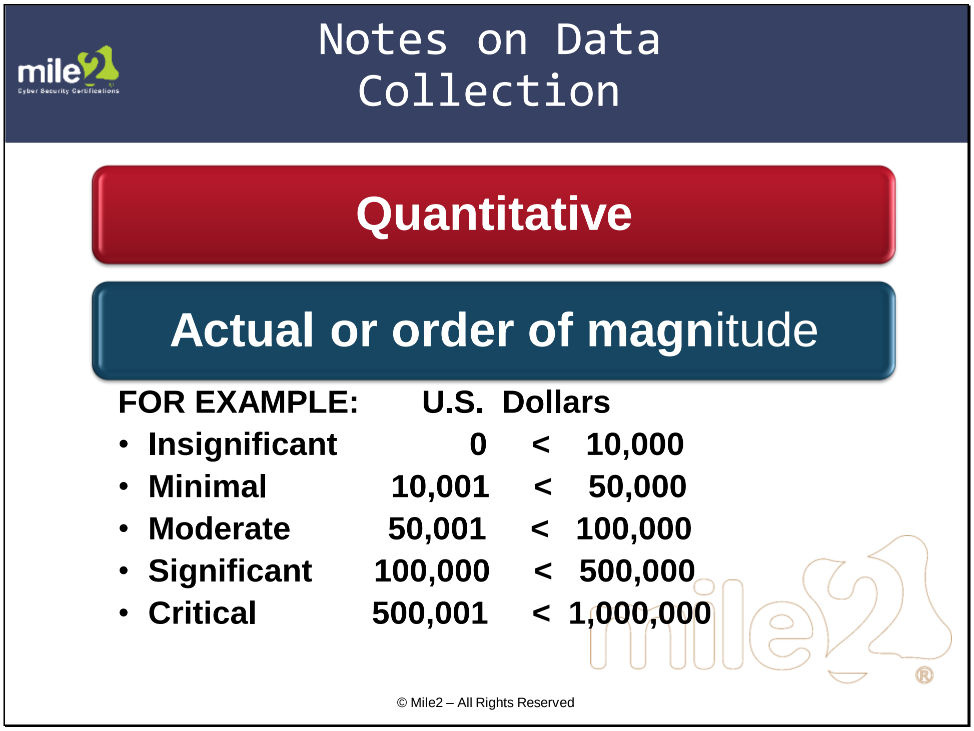
____

____

____

____

Slide 23



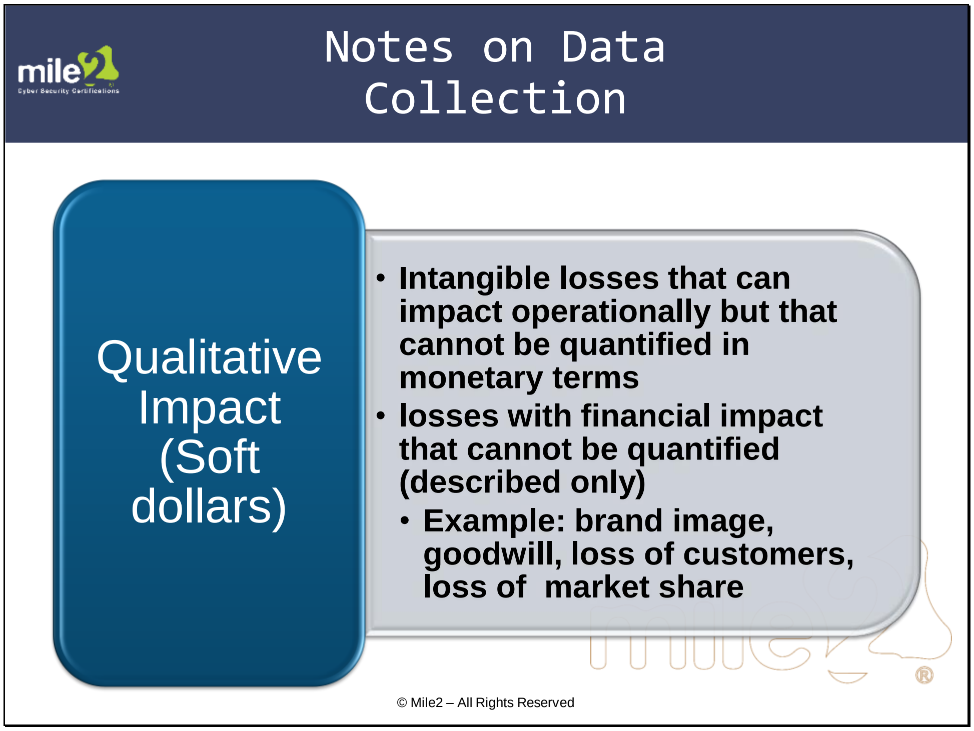
Notes on Data Collection

Quantitative

Actual or order of magnitude

FOR EXAMPLE:	U.S. Dollars		
• Insignificant	0	<	10,000
• Minimal	10,001	<	50,000
• Moderate	50,001	<	100,000
• Significant	100,000	<	500,000
• Critical	500,001	<	1,000,000

Slide 24

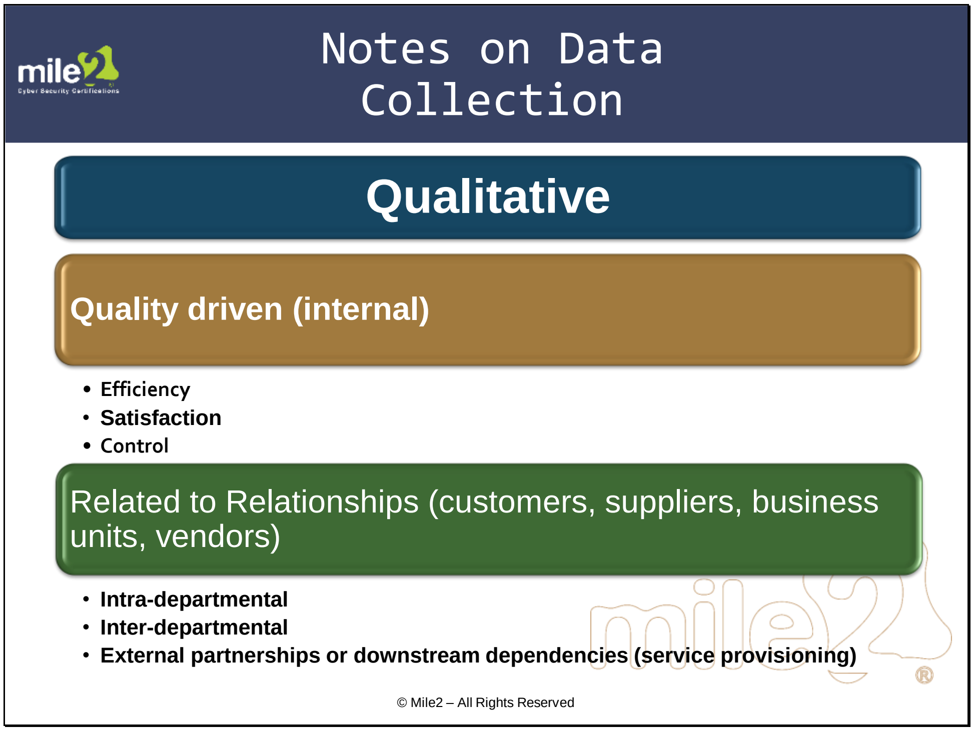


Notes on Data Collection

Qualitative Impact (Soft dollars)

- Intangible losses that can impact operationally but that cannot be quantified in monetary terms
- losses with financial impact that cannot be quantified (described only)
  - Example: brand image, goodwill, loss of customers, loss of market share

Slide 25



Notes on Data Collection

Qualitative

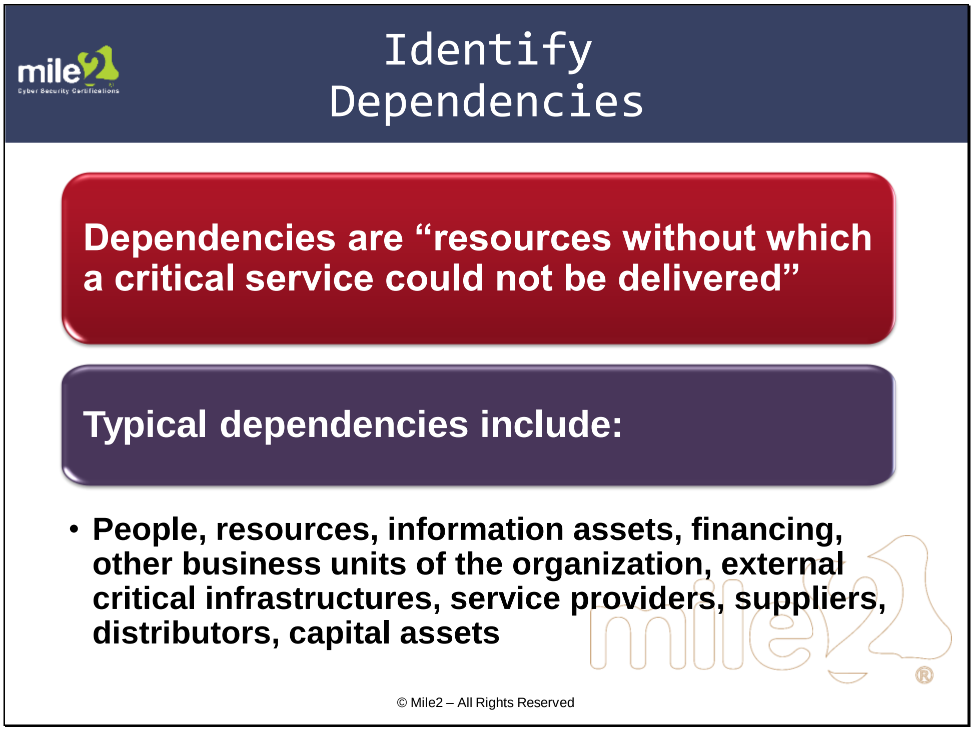
Quality driven (internal)

- Efficiency
- Satisfaction
- Control

Related to Relationships (customers, suppliers, business units, vendors)

- Intra-departmental
- Inter-departmental
- External partnerships or downstream dependencies (service provisioning)

Slide 26



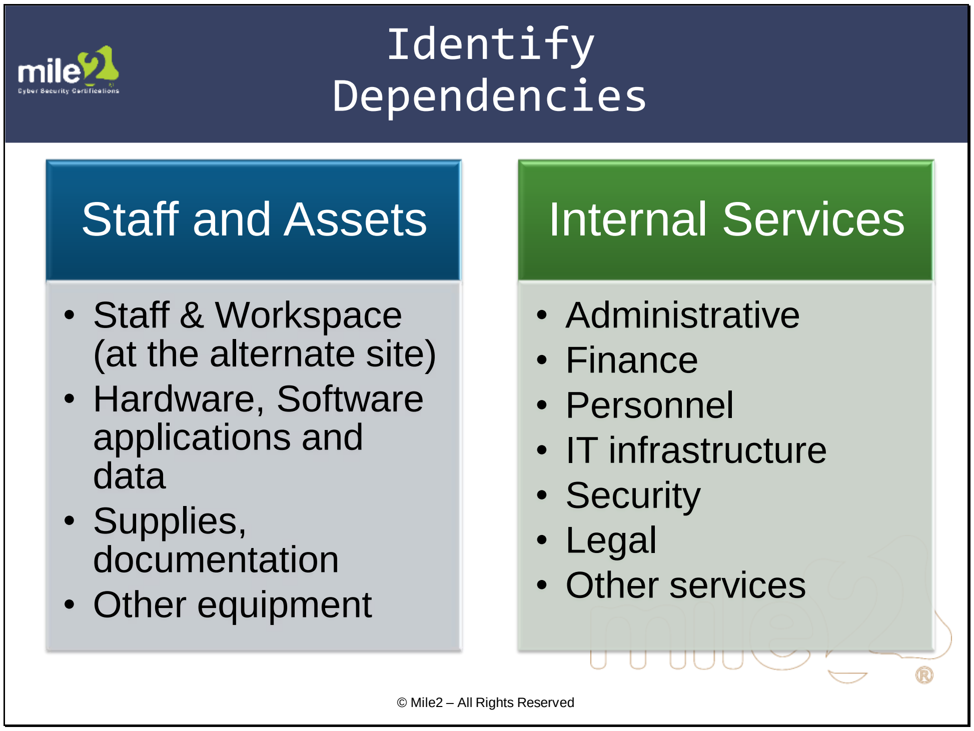
Identify Dependencies

Dependencies are “resources without which a critical service could not be delivered”

Typical dependencies include:

- People, resources, information assets, financing, other business units of the organization, external critical infrastructures, service providers, suppliers, distributors, capital assets

Slide 27



Identify Dependencies

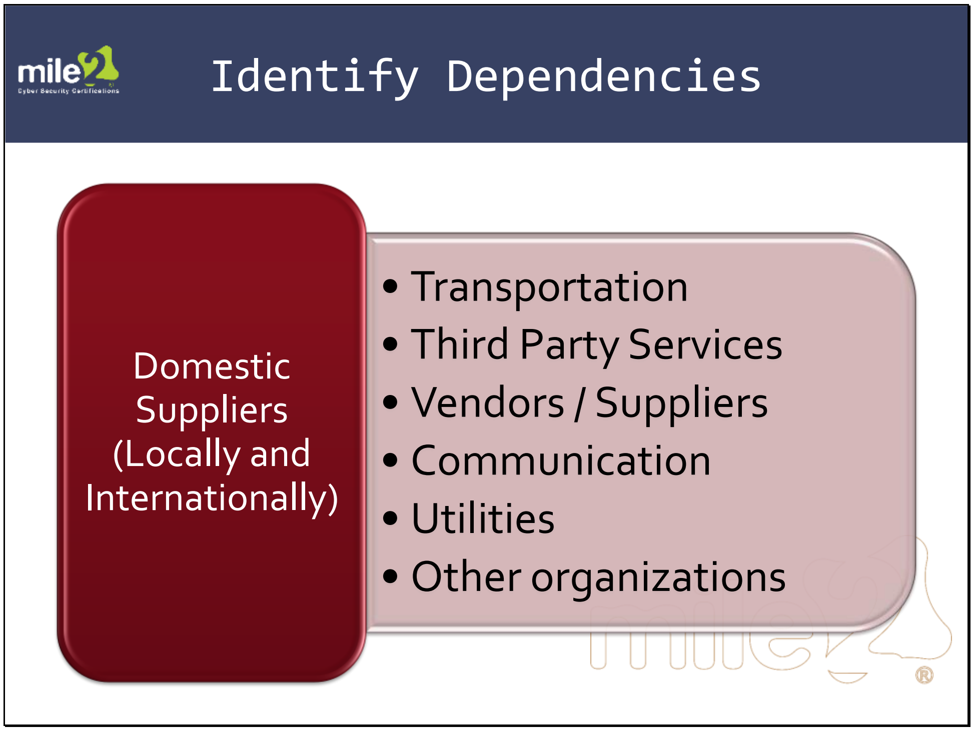
Staff and Assets

- Staff & Workspace (at the alternate site)
- Hardware, Software applications and data
- Supplies, documentation
- Other equipment

Internal Services

- Administrative
- Finance
- Personnel
- IT infrastructure
- Security
- Legal
- Other services

Slide 28

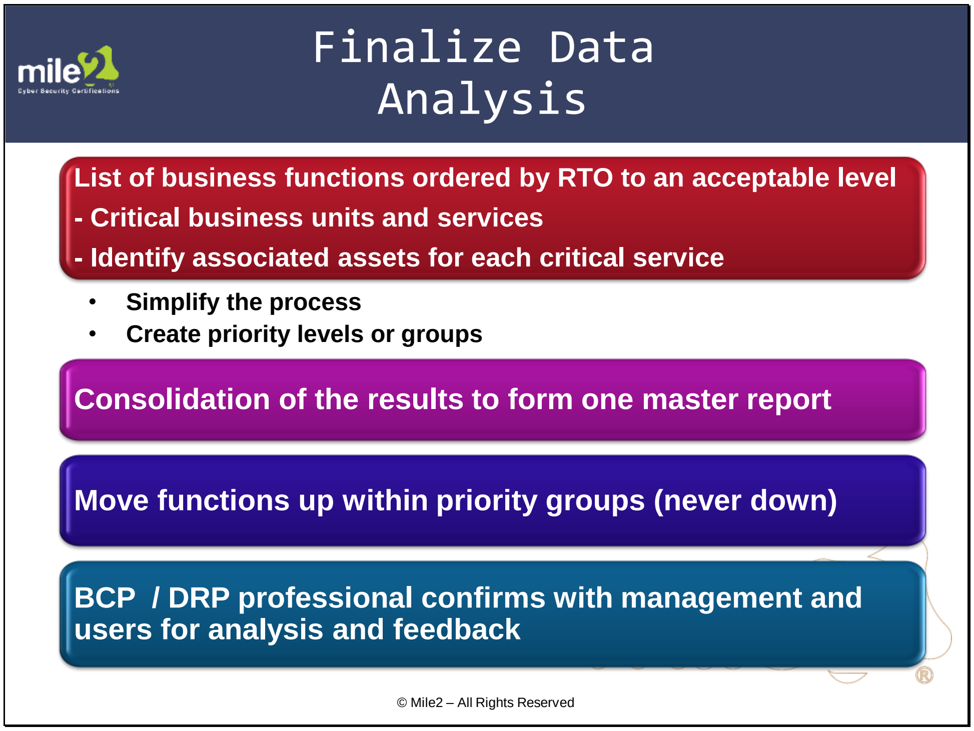


Identify Dependencies

Domestic Suppliers (Locally and Internationally)

- Transportation
- Third Party Services
- Vendors / Suppliers
- Communication
- Utilities
- Other organizations

Slide 29



Finalize Data Analysis

List of business functions ordered by RTO to an acceptable level

- Critical business units and services
- Identify associated assets for each critical service

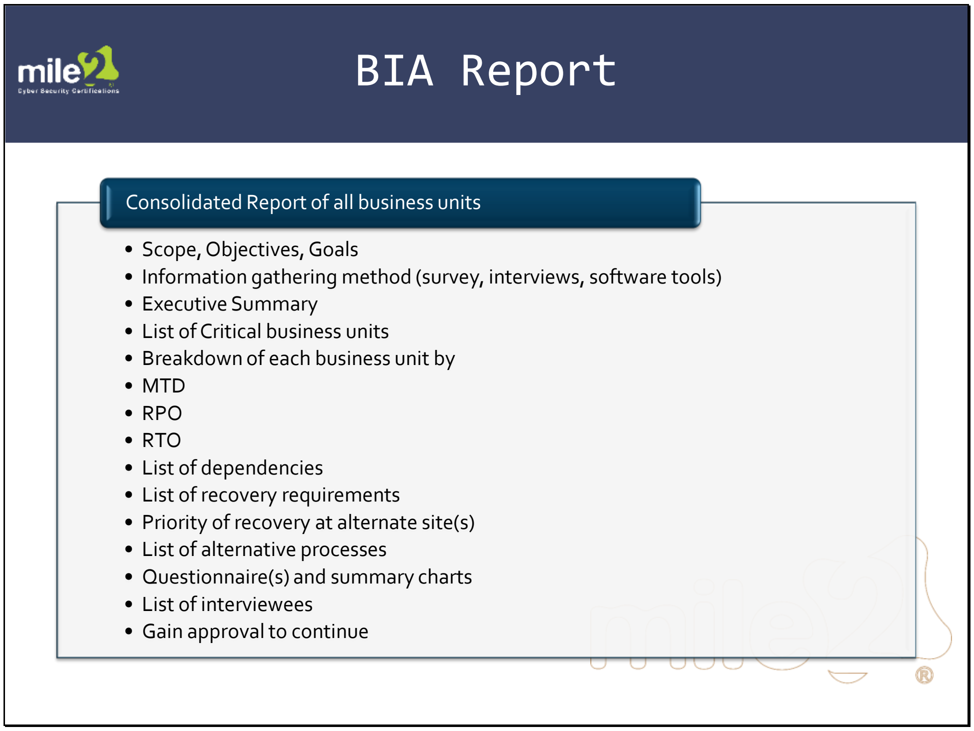
- Simplify the process
- Create priority levels or groups

Consolidation of the results to form one master report

Move functions up within priority groups (never down)

BCP / DRP professional confirms with management and users for analysis and feedback

Slide 30

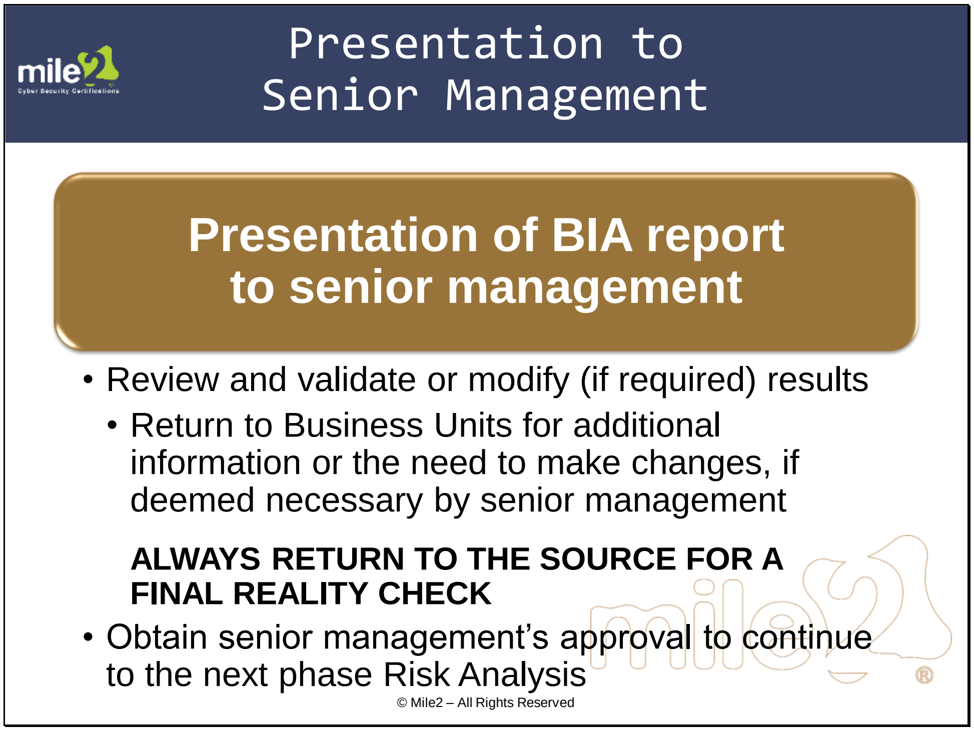


BIA Report

Consolidated Report of all business units

- Scope, Objectives, Goals
- Information gathering method (survey, interviews, software tools)
- Executive Summary
- List of Critical business units
- Breakdown of each business unit by
- MTD
- RPO
- RTO
- List of dependencies
- List of recovery requirements
- Priority of recovery at alternate site(s)
- List of alternative processes
- Questionnaire(s) and summary charts
- List of interviewees
- Gain approval to continue

Slide 31



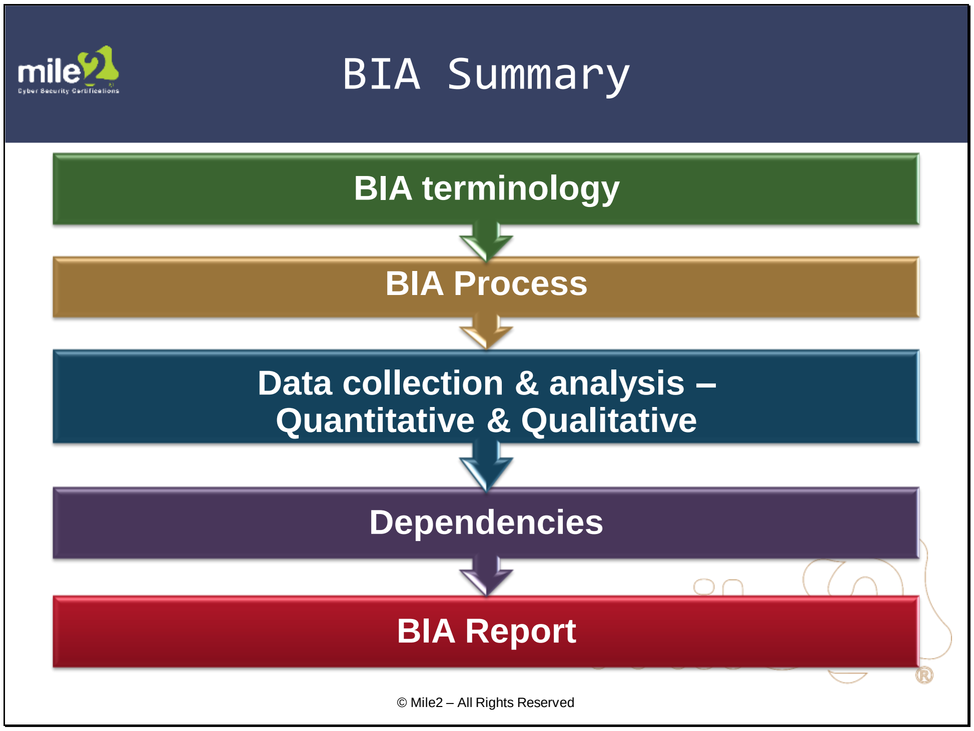
Presentation to Senior Management

Presentation of BIA report to senior management

- Review and validate or modify (if required) results
  - Return to Business Units for additional information or the need to make changes, if deemed necessary by senior management

    ALWAYS RETURN TO THE SOURCE FOR A FINAL REALITY CHECK
- Obtain senior management's approval to continue to the next phase Risk Analysis

Slide 32



BIA Summary

BIA terminology

BIA Process

Data collection & analysis – Quantitative & Qualitative

Dependencies

BIA Report

Slide 33

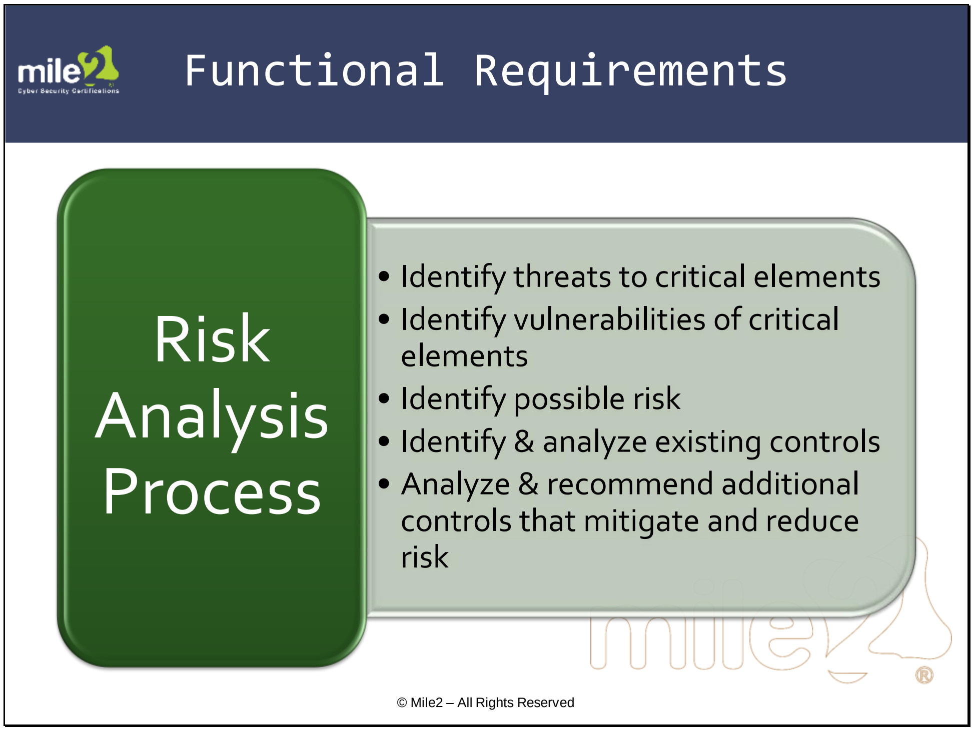
mile2

Cyber Security Certifications

Risk Analysis

Section 2

Slide 34

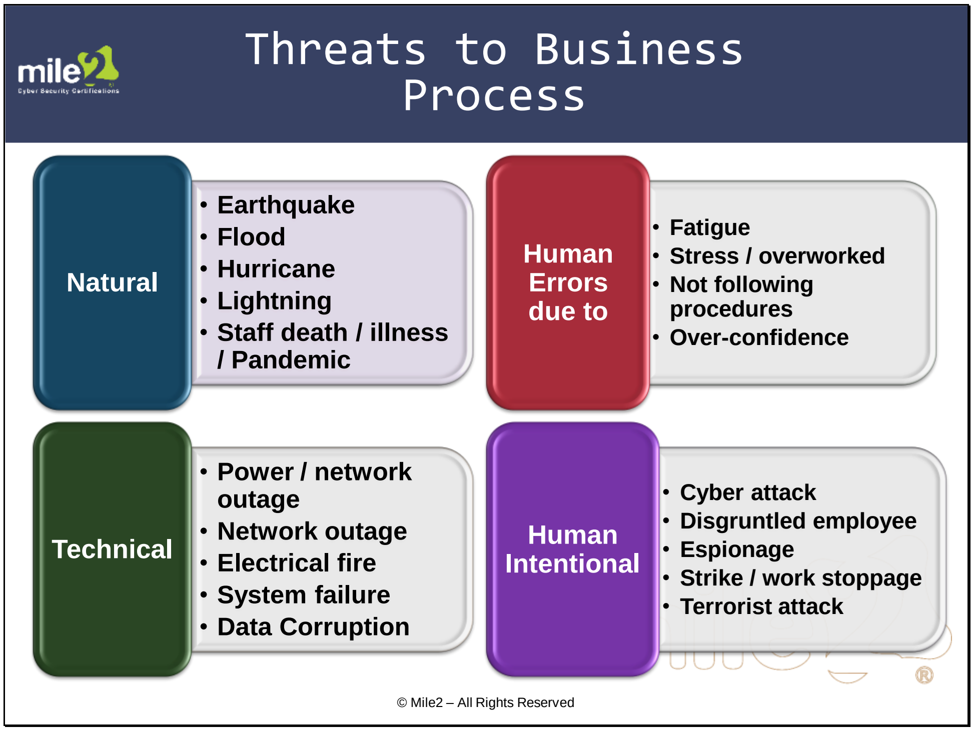


Functional Requirements

Risk Analysis Process

- Identify threats to critical elements
- Identify vulnerabilities of critical elements
- Identify possible risk
- Identify & analyze existing controls
- Analyze & recommend additional controls that mitigate and reduce risk

Slide 35



Threats to Business Process

Natural

- Earthquake
- Flood
- Hurricane
- Lightning
- Staff death / illness / Pandemic

Human Errors due to

- Fatigue
- Stress / overworked
- Not following procedures
- Over-confidence

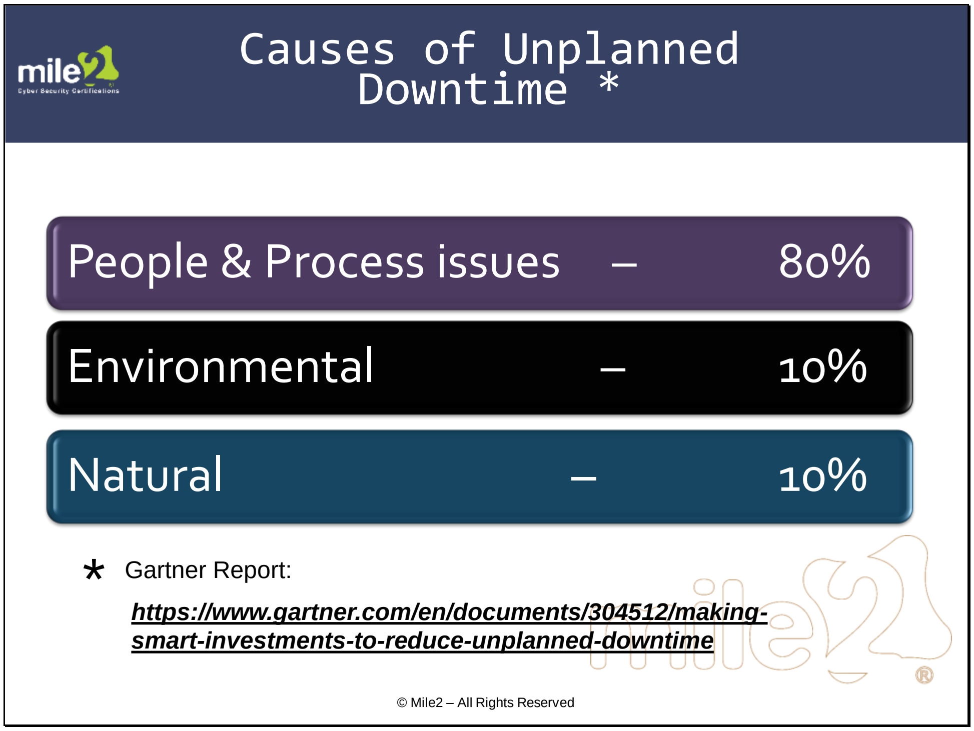
Technical

- Power / network outage
- Network outage
- Electrical fire
- System failure
- Data Corruption

Human Intentional

- Cyber attack
- Disgruntled employee
- Espionage
- Strike / work stoppage
- Terrorist attack

Slide 36



Causes of Unplanned Downtime *

People & Process issues – 80%

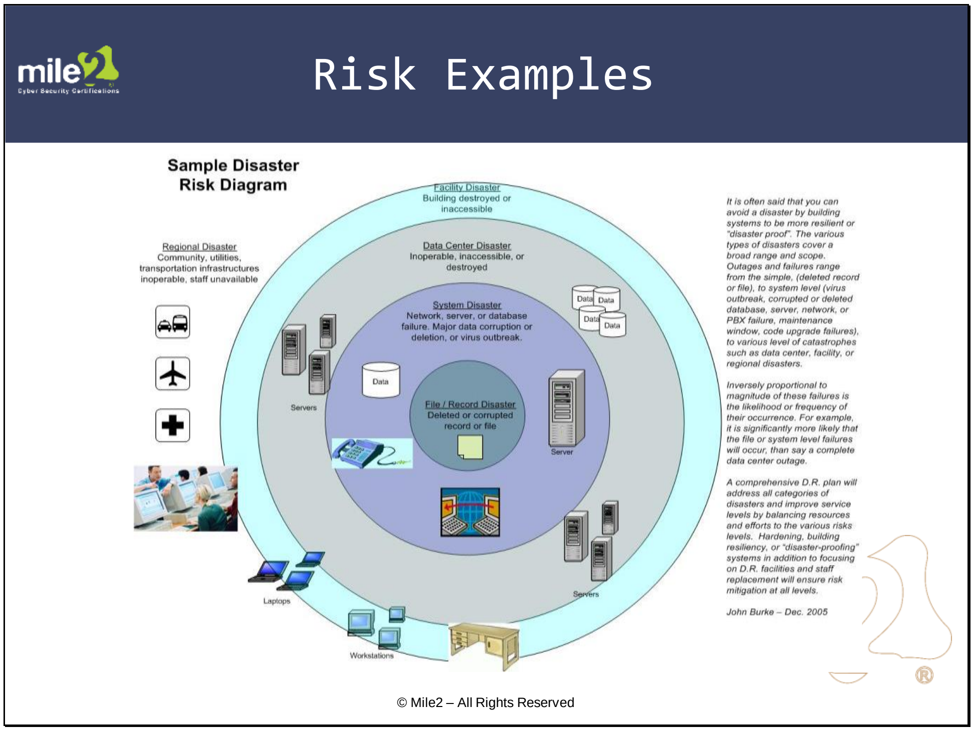
Environmental – 10%

Natural – 10%

* Gartner Report:

https://www.gartner.com/en/documents/304512/making-smart-investments-to-reduce-unplanned-downtime

Slide 37



Risk Examples

Sample Disaster Risk Diagram

Facility Disaster
Building destroyed or inaccessible

Regional Disaster
Community, utilities, transportation infrastructures inoperable, staff unavailable

Data Center Disaster
Inoperable, inaccessible, or destroyed

System Disaster
Network, server, or database failure. Major data corruption or deletion, or virus outbreak.

File / Record Disaster
Deleted or corrupted record or file

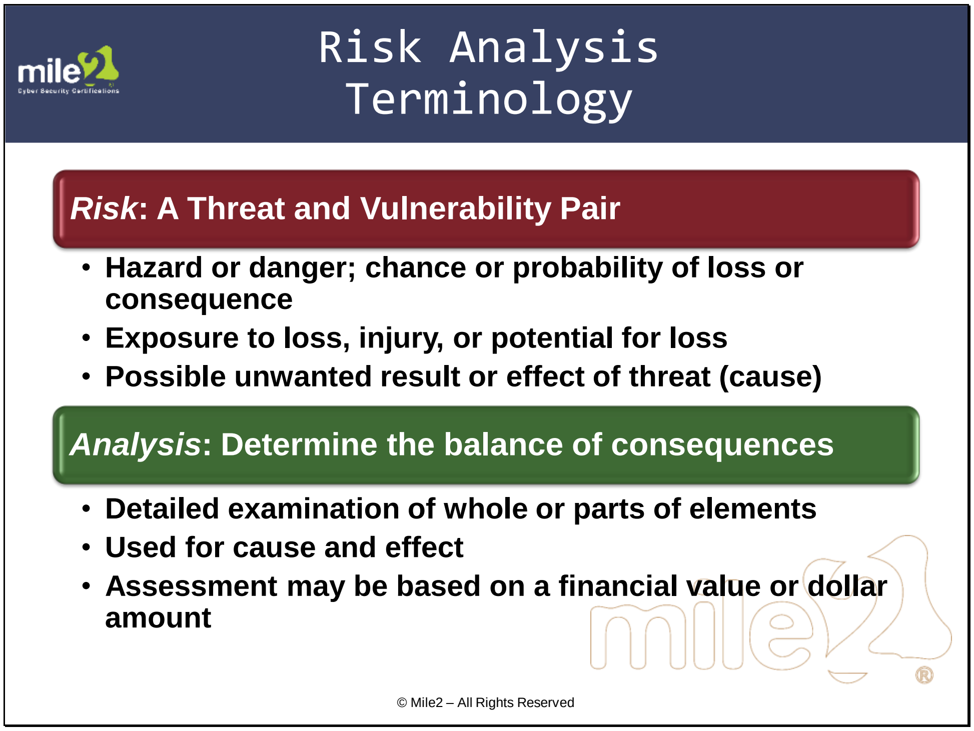
It is often said that you can avoid a disaster by building systems to be more resilient or "disaster proof". The various types of disasters cover a broad range and scope. Outages and failures range from the simple, (deleted record or file), to system level (virus outbreak, corrupted or deleted database, server, network, or PBX failure, maintenance window, code upgrade failures), to various level of catastrophes such as data center, facility, or regional disasters.

Inversely proportional to magnitude of these failures is the likelihood or frequency of their occurrence. For example, it is significantly more likely that the file or system level failures will occur, than say a complete data center outage.

A comprehensive D.R. plan will address all categories of disasters and improve service levels by balancing resources and efforts to the various risks levels. Hardening, building resiliency, or "disaster-proofing" systems in addition to focusing on D.R. facilities and staff replacement will ensure risk mitigation at all levels.

John Burke – Dec. 2005

Slide 38



Risk Analysis Terminology

***Risk*: A Threat and Vulnerability Pair**

- **Hazard or danger; chance or probability of loss or consequence**
- **Exposure to loss, injury, or potential for loss**
- **Possible unwanted result or effect of threat (cause)**

***Analysis*: Determine the balance of consequences**

- **Detailed examination of whole or parts of elements**
- **Used for cause and effect**
- **Assessment may be based on a financial value or dollar amount**

____

____

____

____

____

____

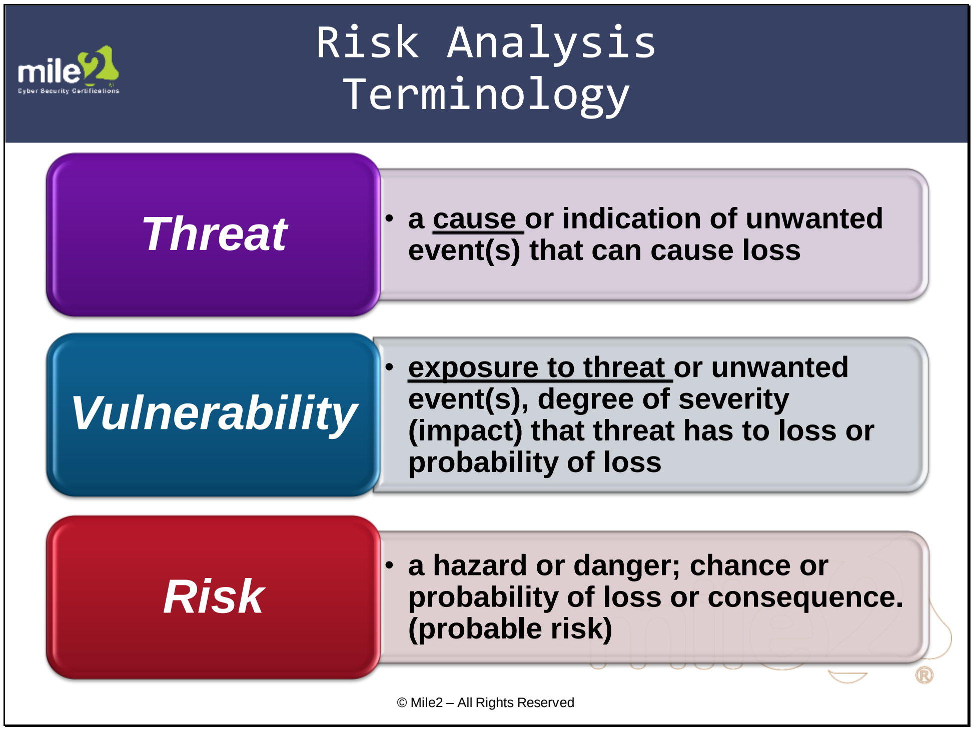
____

____

____

____

Slide 39



Risk Analysis Terminology

Threat

- a cause or indication of unwanted event(s) that can cause loss

Vulnerability

- exposure to threat or unwanted event(s), degree of severity (impact) that threat has to loss or probability of loss

Risk

- a hazard or danger; chance or probability of loss or consequence. (probable risk)

____

____

____

____

____

____

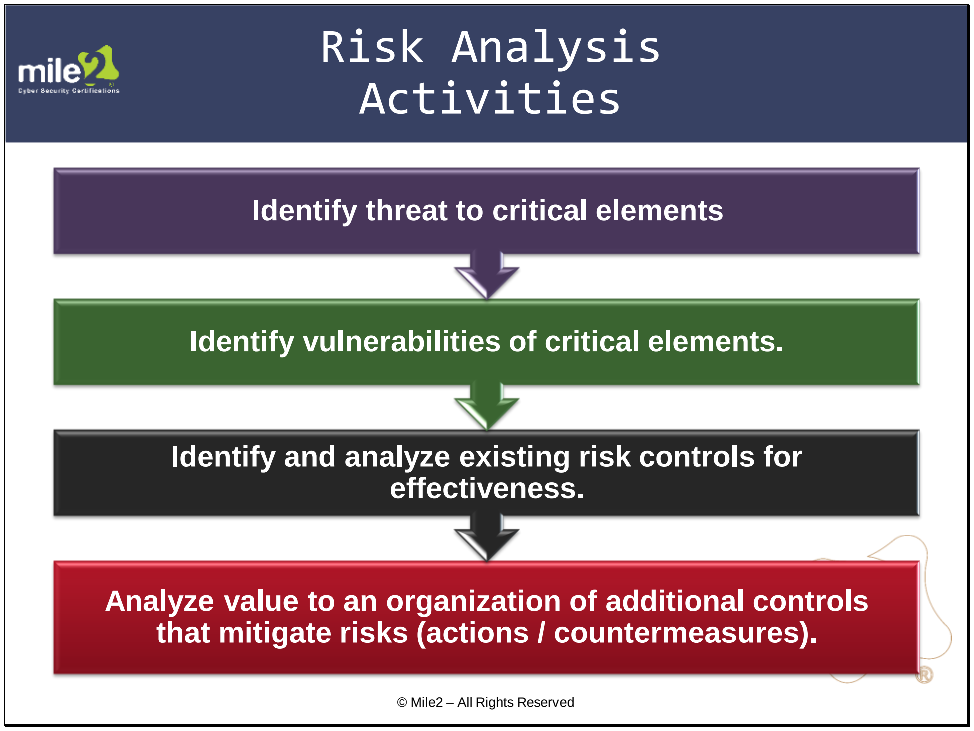
____

____

____

____

Slide 40



Risk Analysis Activities

Identify threat to critical elements

Identify vulnerabilities of critical elements.

Identify and analyze existing risk controls for effectiveness.

Analyze value to an organization of additional controls that mitigate risks (actions / countermeasures).

© Mile2 – All Rights Reserved

____

____

____

____

____

____

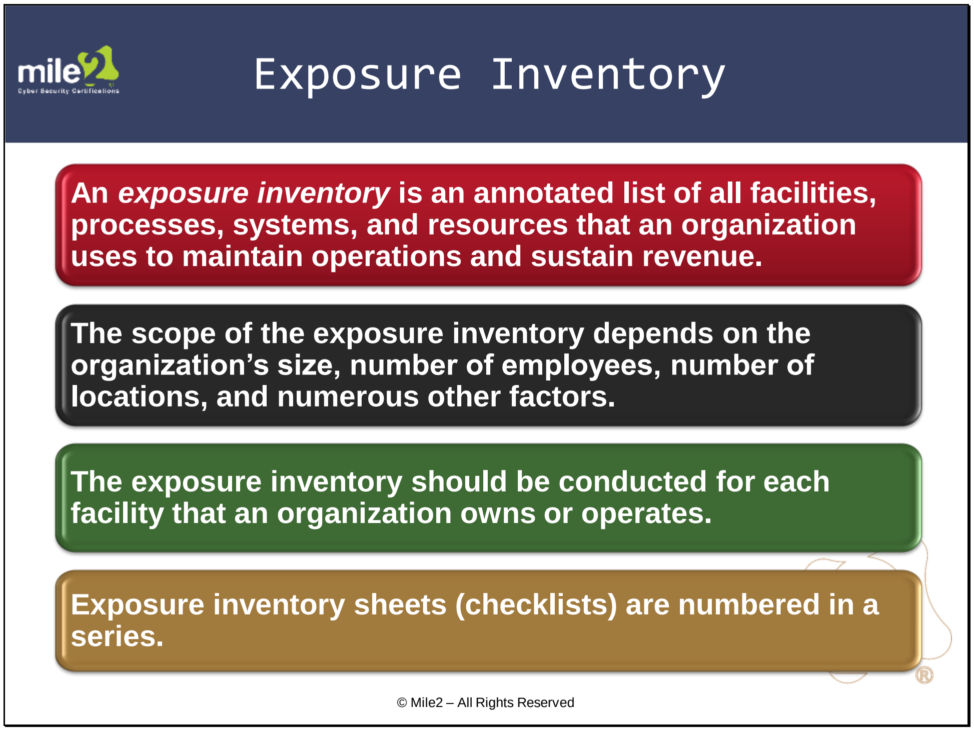
____

____

____

____

Slide 41



Exposure Inventory

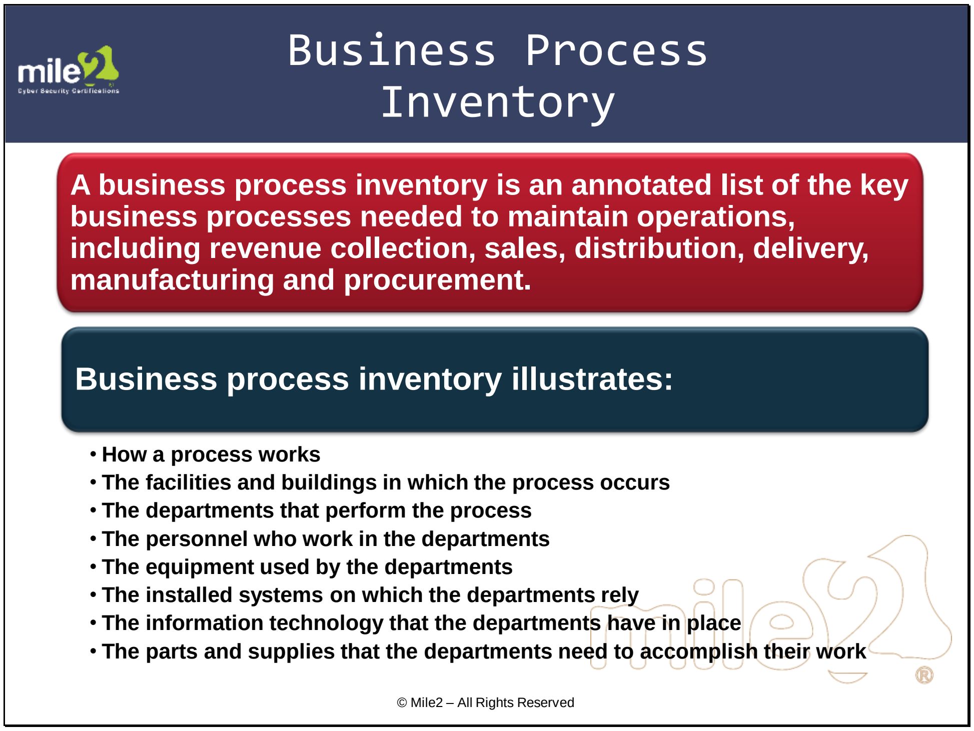
An *exposure inventory* is an annotated list of all facilities, processes, systems, and resources that an organization uses to maintain operations and sustain revenue.

The scope of the exposure inventory depends on the organization's size, number of employees, number of locations, and numerous other factors.

The exposure inventory should be conducted for each facility that an organization owns or operates.

Exposure inventory sheets (checklists) are numbered in a series.

Slide 42



Business Process Inventory

A business process inventory is an annotated list of the key business processes needed to maintain operations, including revenue collection, sales, distribution, delivery, manufacturing and procurement.

Business process inventory illustrates:

- How a process works
- The facilities and buildings in which the process occurs
- The departments that perform the process
- The personnel who work in the departments
- The equipment used by the departments
- The installed systems on which the departments rely
- The information technology that the departments have in place
- The parts and supplies that the departments need to accomplish their work

____

____

____

____

____

____

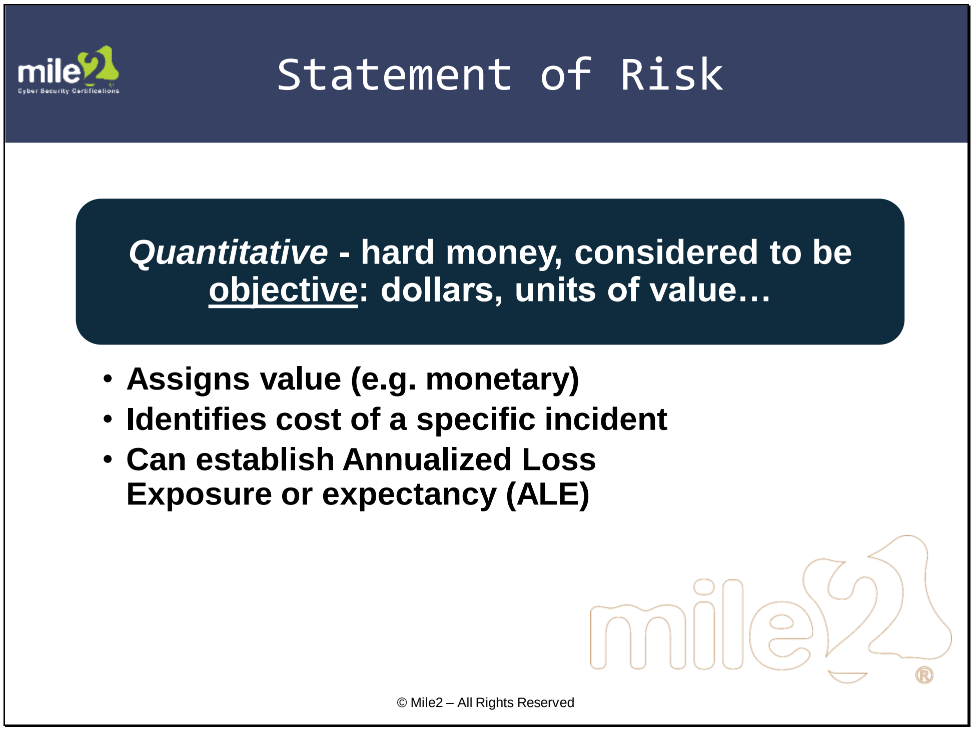
____

____

____

____

Slide 43

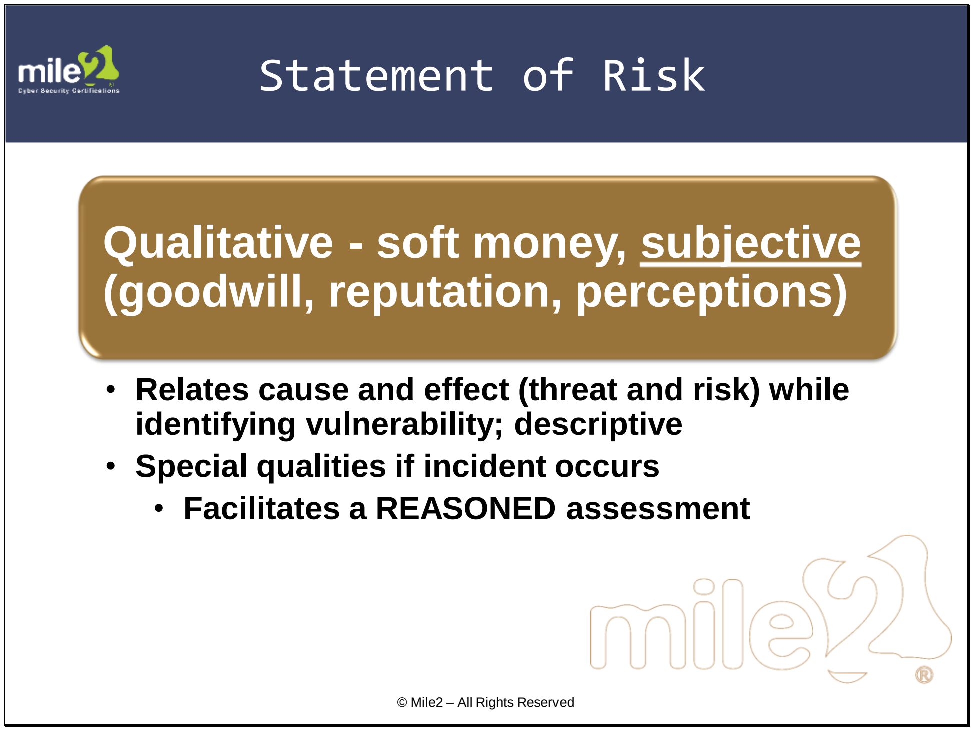


Statement of Risk

Quantitative **- hard money, considered to be objective: dollars, units of value…**

- **Assigns value (e.g. monetary)**
- **Identifies cost of a specific incident**
- **Can establish Annualized Loss Exposure or expectancy (ALE)**

Slide 44

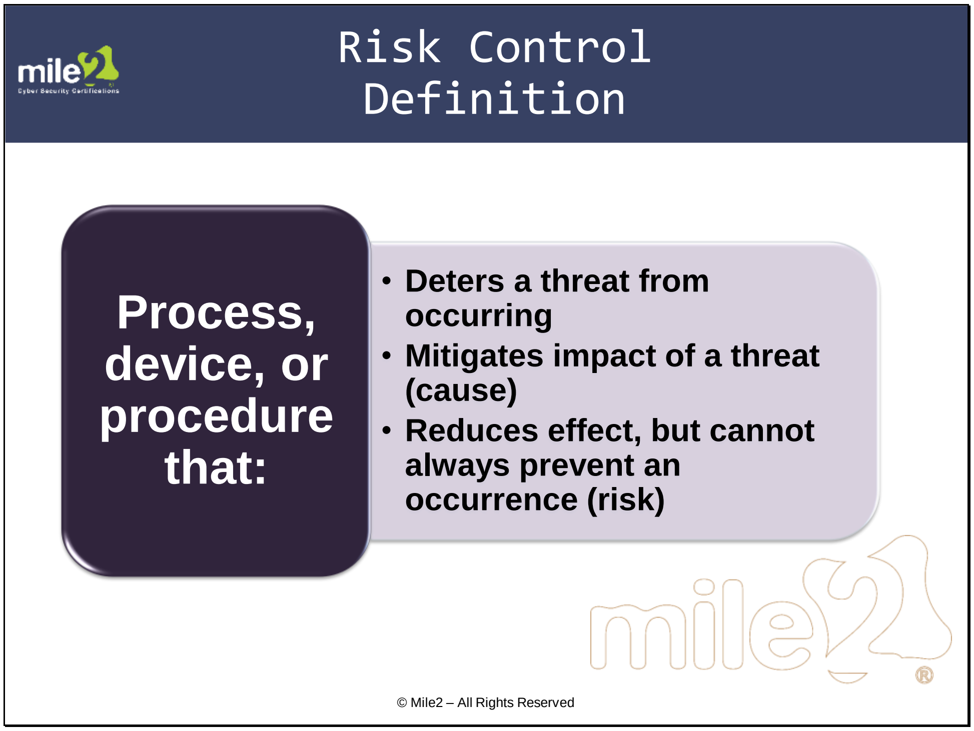


Statement of Risk

Qualitative - soft money, subjective (goodwill, reputation, perceptions)

- **Relates cause and effect (threat and risk) while identifying vulnerability; descriptive**
- **Special qualities if incident occurs**
  - **Facilitates a REASONED assessment**

Slide 45



Risk Control Definition

Process, device, or procedure that:

- **Deters a threat from occurring**
- **Mitigates impact of a threat (cause)**
- **Reduces effect, but cannot always prevent an occurrence (risk)**

____

____

____

____

____

____

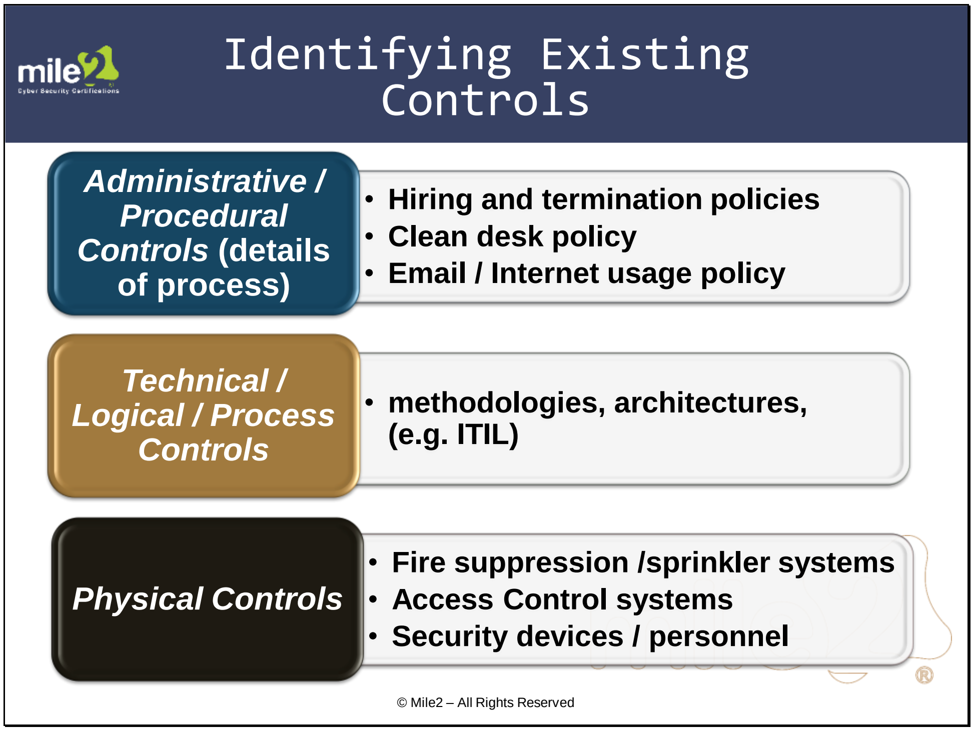
____

____

____

____

Slide 46



Identifying Existing Controls

***Administrative / Procedural Controls* (details of process)**

- **Hiring and termination policies**
- **Clean desk policy**
- **Email / Internet usage policy**

Technical / Logical / Process Controls

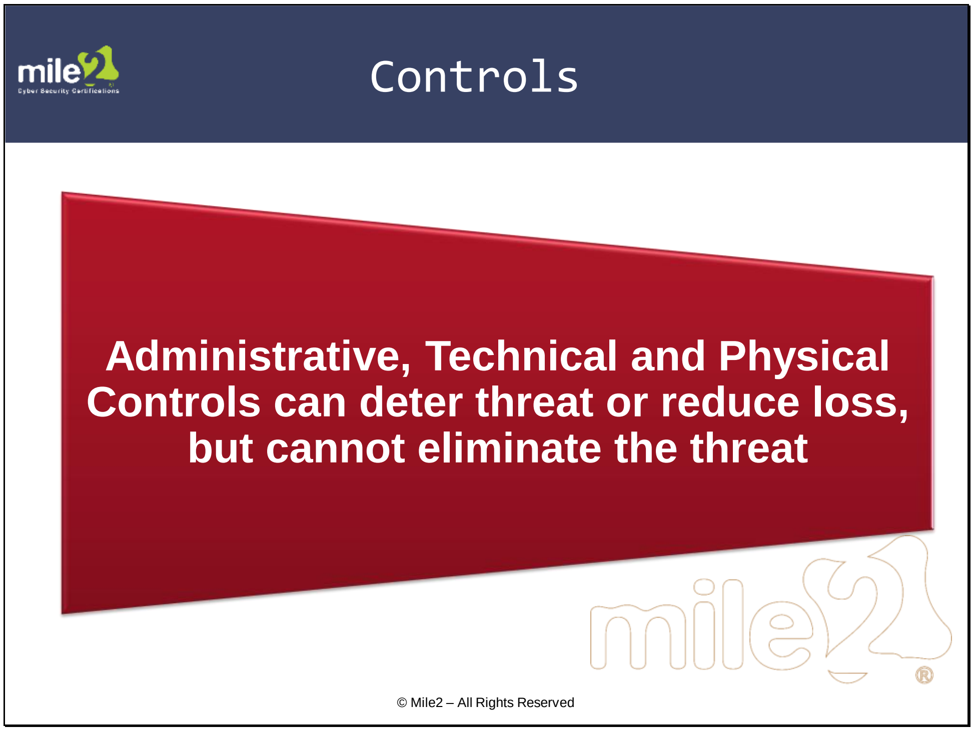
- **methodologies, architectures, (e.g. ITIL)**

Physical Controls

- **Fire suppression /sprinkler systems**
- **Access Control systems**
- **Security devices / personnel**

© Mile2 – All Rights Reserved

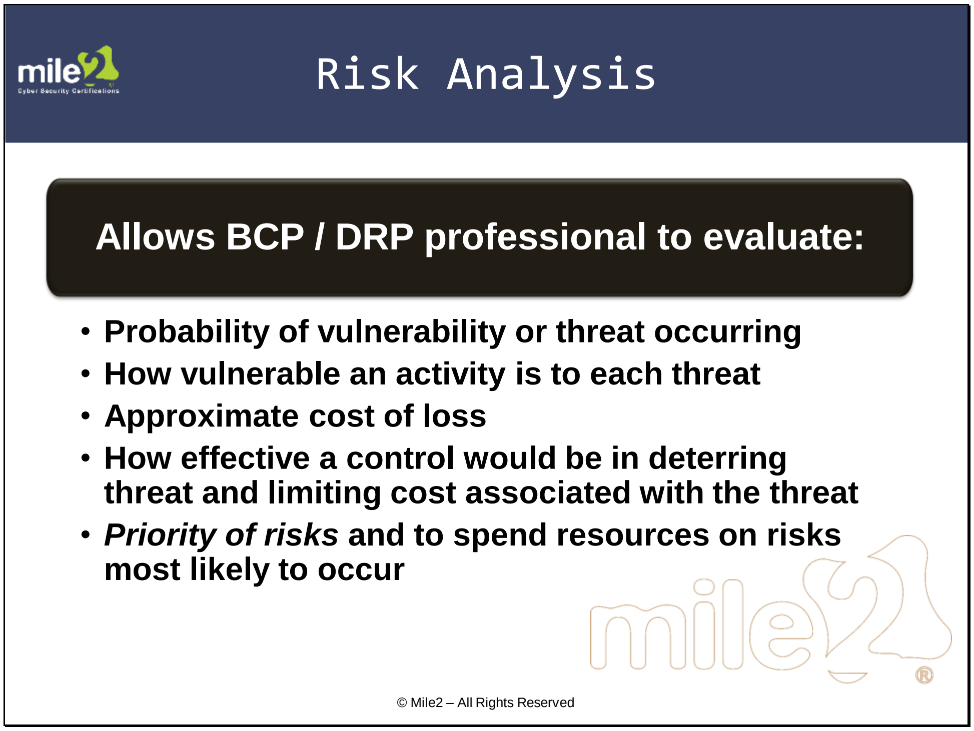
Slide 47



Controls

Administrative, Technical and Physical Controls can deter threat or reduce loss, but cannot eliminate the threat

Slide 48

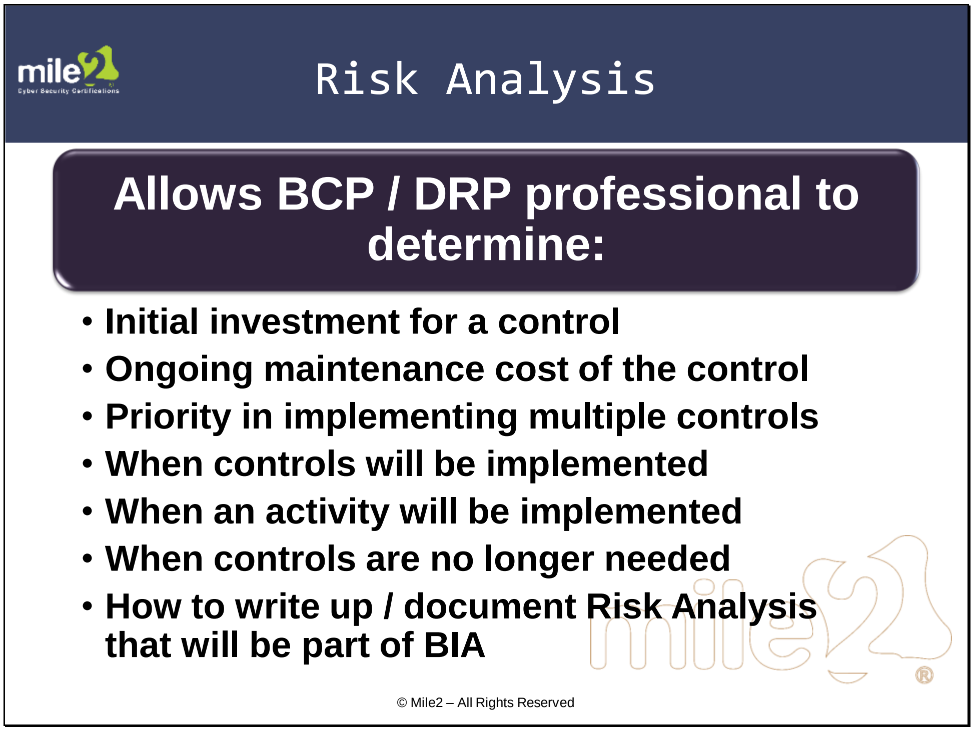


Risk Analysis

Allows BCP / DRP professional to evaluate:

- **Probability of vulnerability or threat occurring**
- **How vulnerable an activity is to each threat**
- **Approximate cost of loss**
- **How effective a control would be in deterring threat and limiting cost associated with the threat**
- ***Priority of risks* and to spend resources on risks most likely to occur**

Slide 49

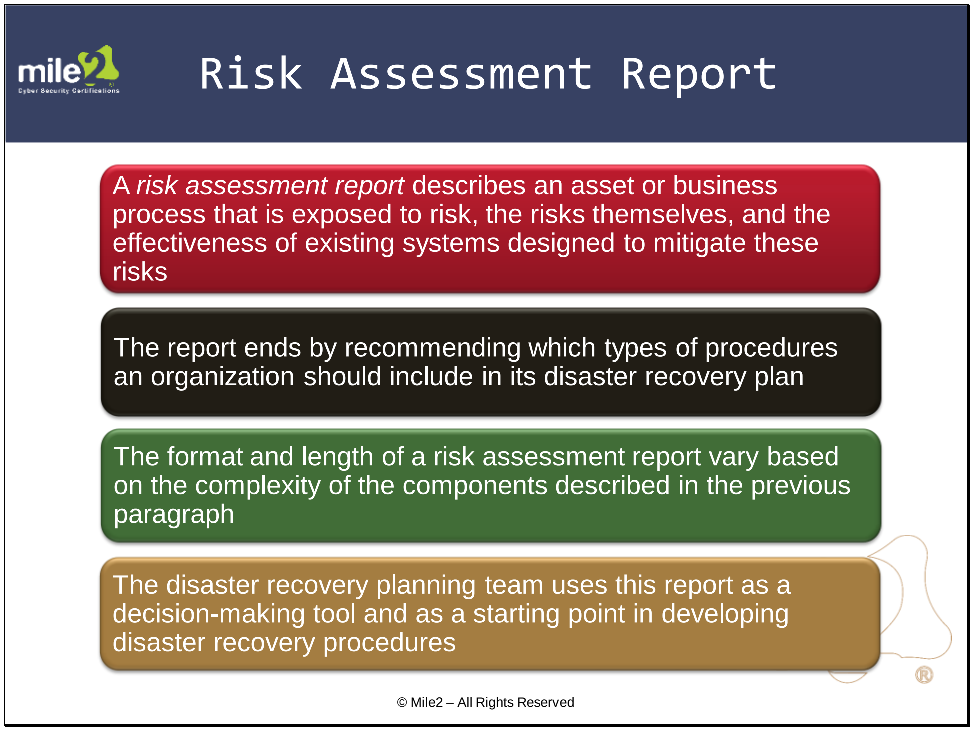


Risk Analysis

Allows BCP / DRP professional to determine:

- Initial investment for a control
- Ongoing maintenance cost of the control
- Priority in implementing multiple controls
- When controls will be implemented
- When an activity will be implemented
- When controls are no longer needed
- How to write up / document Risk Analysis that will be part of BIA

Slide 50



Risk Assessment Report

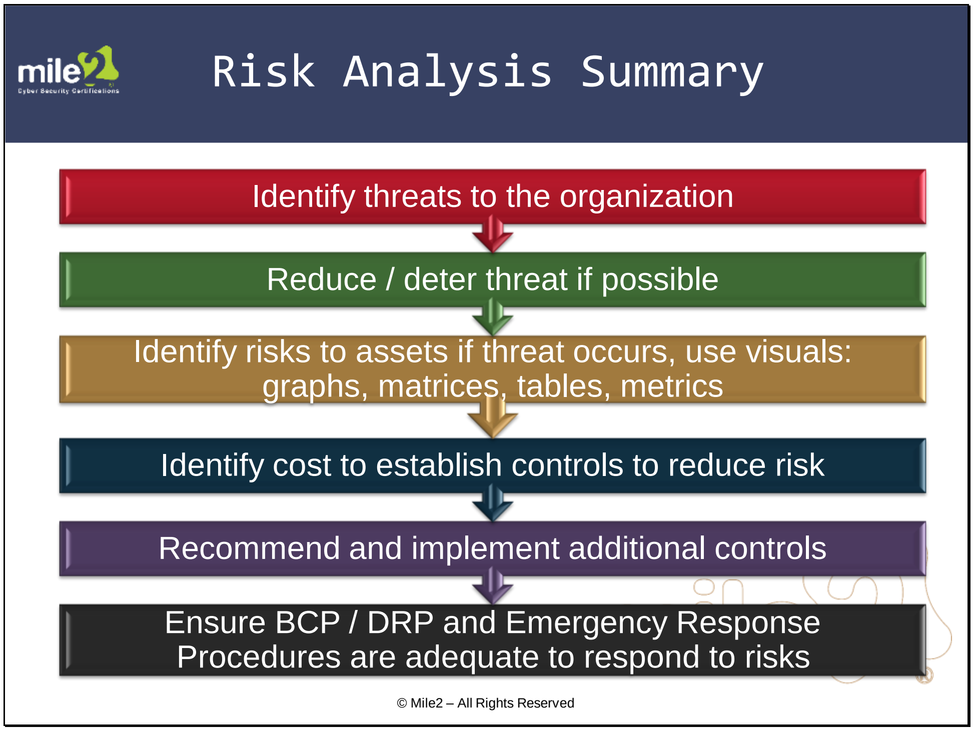
A *risk assessment report* describes an asset or business process that is exposed to risk, the risks themselves, and the effectiveness of existing systems designed to mitigate these risks

The report ends by recommending which types of procedures an organization should include in its disaster recovery plan

The format and length of a risk assessment report vary based on the complexity of the components described in the previous paragraph

The disaster recovery planning team uses this report as a decision-making tool and as a starting point in developing disaster recovery procedures

Slide 51



Risk Analysis Summary

Identify threats to the organization

Reduce / deter threat if possible

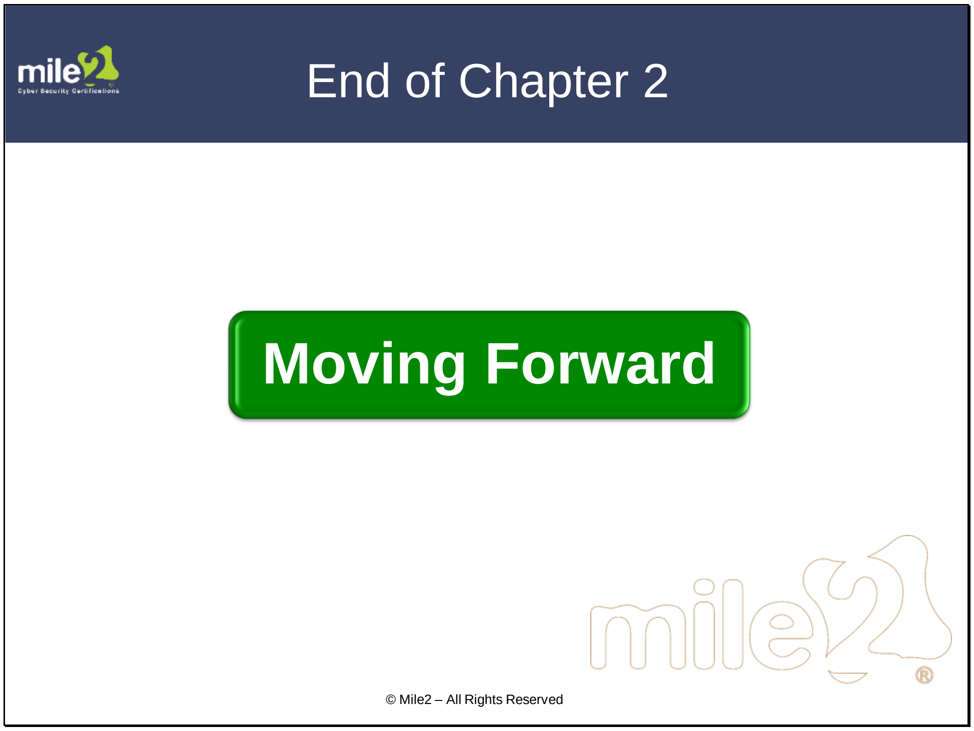
Identify risks to assets if threat occurs, use visuals: graphs, matrices, tables, metrics

Identify cost to establish controls to reduce risk

Recommend and implement additional controls

Ensure BCP / DRP and Emergency Response Procedures are adequate to respond to risks

Slide 52



End of Chapter 2

Moving Forward

Questions and Answers

Review Questions:

1. True or False: Business Impact Analysis (BIA) is an analysis that assesses the quantitative and qualitative impacts and loss that might result if that organization were to suffer a major interruption.
   A. True
   B. False

2. True or False: Maximum Tolerable Downtime (MTD) is the longest amount of time that the business unit can be unavailable before it threatens the survival of the business.
   A. True
   B. False

3. What does “RTO” stand for?
   A. Real Total Outage
   B. Recovery Total Outage
   C. Recovery Time Objective
   D. Recovery Test Objective

4. The Recovery Point Objective is the point in time to which you must recover data. Who in the organization initially determines this?
   A. The Business Owner
   B. The Business Recovery Coordinator
   C. Executive Management
   D. IT Security

5. Which of the following are included in Business Impact Analysis (BIA)?
   A. Determine Maximum Tolerable Downtime (MTD)
   B. Determine maximum tolerable data loss (Recovery Point Objective – RPO)
   C. Determine staffing levels in “DR Mode”
   D. Determine recovery priorities
   E. All of the above

Answer Key:

1. A
   True. Business Impact Analysis (BIA) is an analysis that assesses the quantitative and qualitative impacts and loss that might result if that organization were to suffer a major interruption.

2. A
   True. Maximum Tolerable Downtime (MTD) is the longest amount of time that the business unit can be unavailable before it threatens the survival of the business.

3. C
   RTO stands for Recovery Time Objective.

4. A
   The Business owner initially determines the point in time to which you must recover data.

5. E
   All of the options listed are included in the Business Impact Analysis.