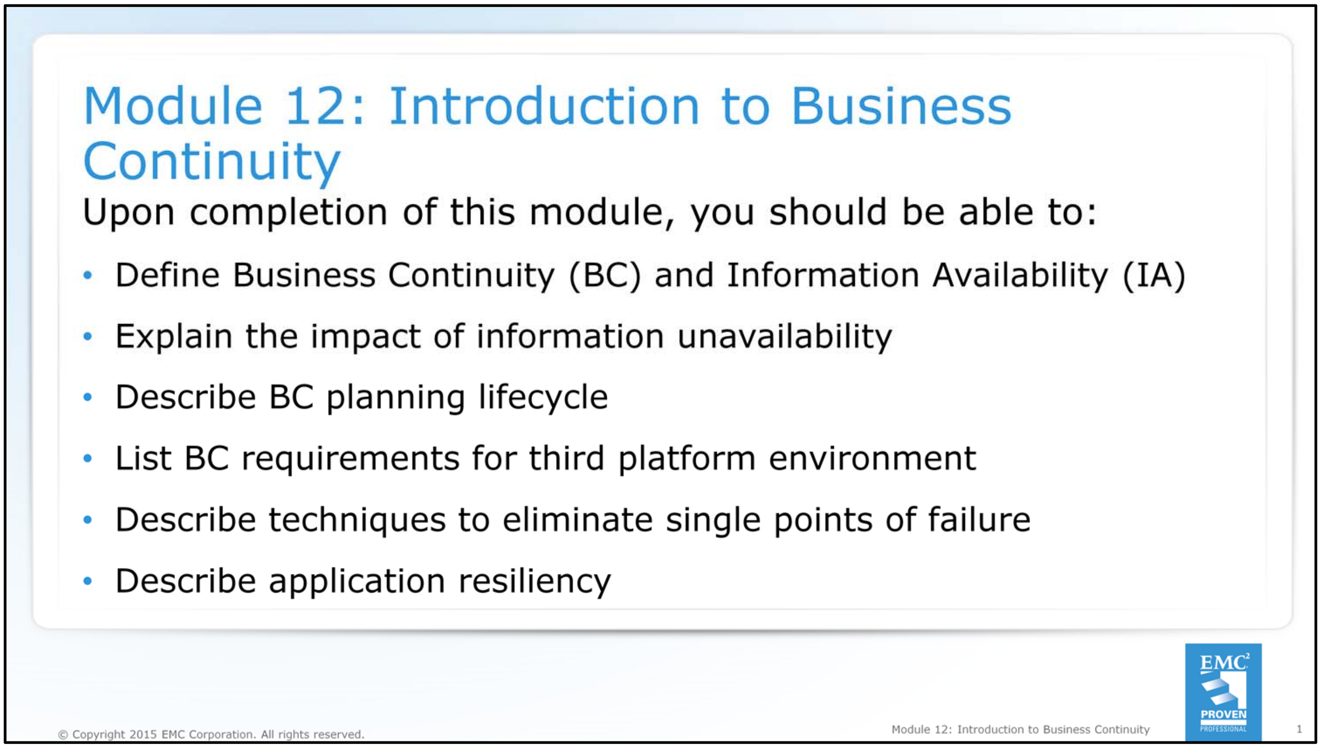


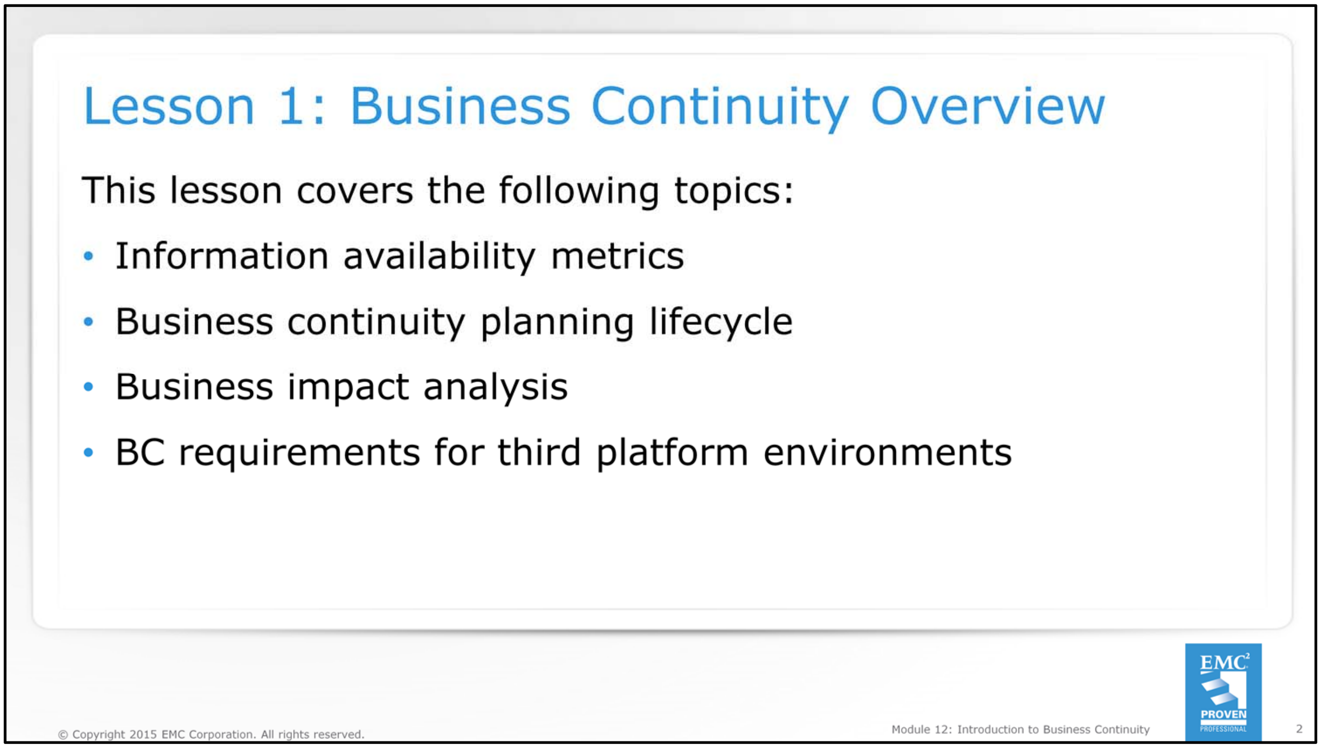
Module 12: Introduction to Business Continuity

Upon completion of this module, you should be able to:

- Define Business Continuity (BC) and Information Availability (IA)
- Explain the impact of information unavailability
- Describe BC planning lifecycle
- List BC requirements for third platform environment
- Describe techniques to eliminate single points of failure
- Describe application resiliency

Module 12: Introduction to Business Continuity 1

This module focuses on business continuity and information availability. This module also focuses on causes and impact of information unavailability. Further, this module focuses on BC planning lifecycle, BC requirements for third platform, BC technology solutions, specifically on eliminating single points of failure and application resiliency.



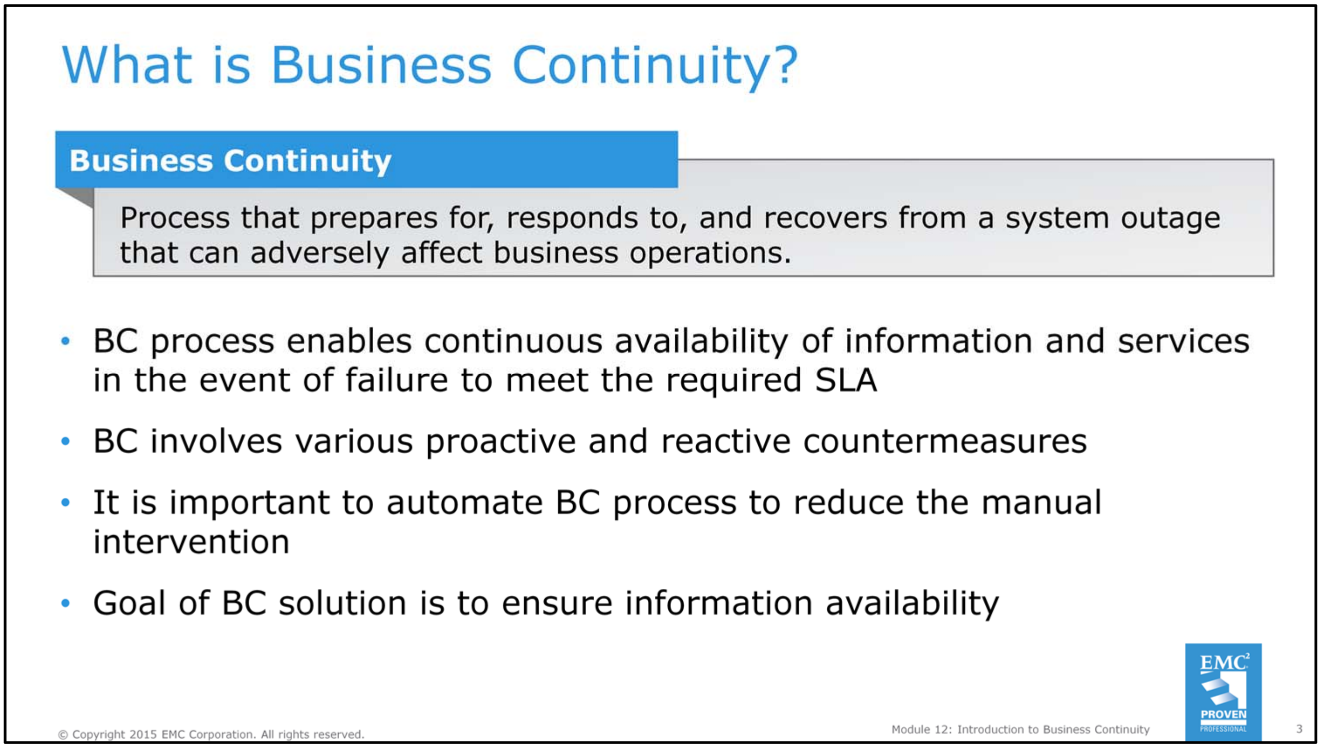
Lesson 1: Business Continuity Overview

This lesson covers the following topics:

- Information availability metrics
- Business continuity planning lifecycle
- Business impact analysis
- BC requirements for third platform environments

Module 12: Introduction to Business Continuity 2

This lesson covers the importance of business continuity to an organization, the factors that can affect information availability and the consequences of information unavailability. This lesson also covers information availability metrics namely mean time between failure (MTBF) and mean time to repair (MTTR). Further this lesson covers business continuity planning lifecycle and business impact analysis. Finally, this lesson covers the BC requirements for third platform environments.



What is Business Continuity?

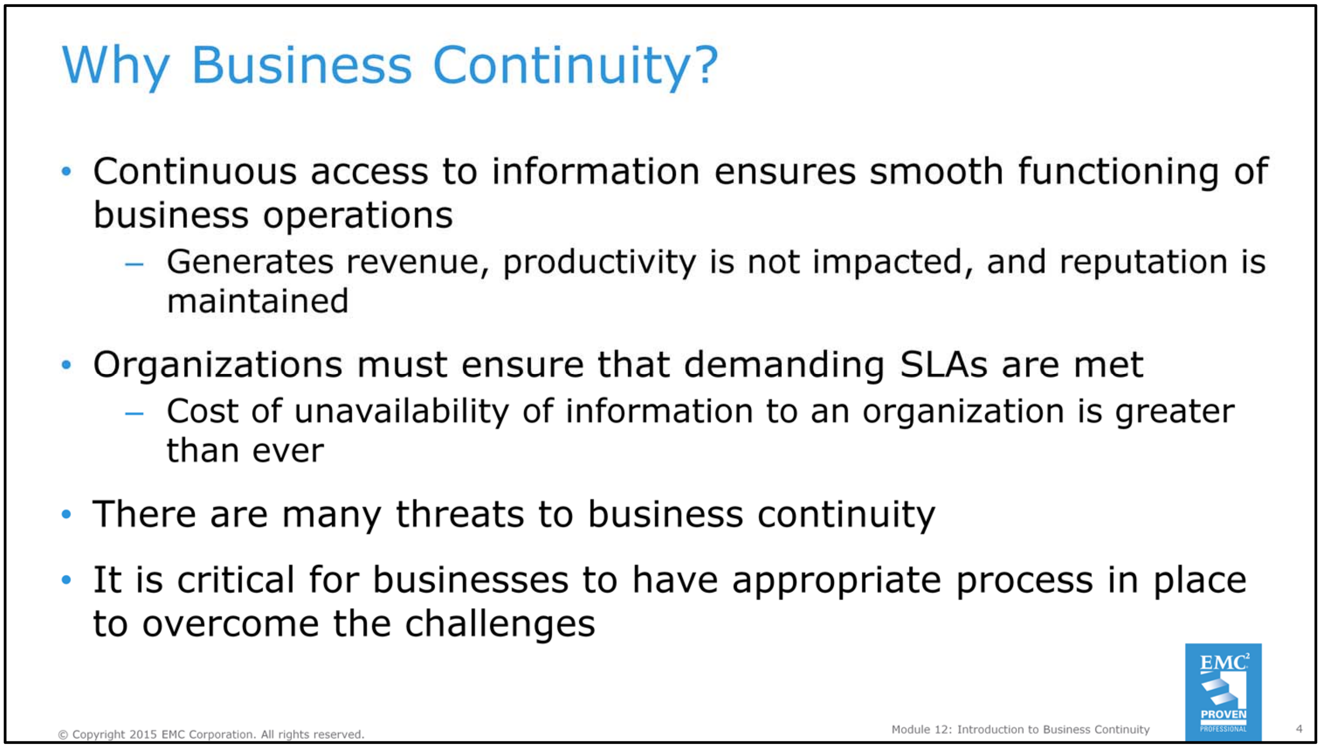
Business Continuity

Process that prepares for, responds to, and recovers from a system outage that can adversely affect business operations.

- BC process enables continuous availability of information and services in the event of failure to meet the required SLA
- BC involves various proactive and reactive countermeasures
- It is important to automate BC process to reduce the manual intervention
- Goal of BC solution is to ensure information availability

Module 12: Introduction to Business Continuity 3

Business continuity (BC) is a set of processes that includes all activities that a business must perform to mitigate the impact of planned and unplanned downtime. BC entails preparing for, responding to, and recovering from a system outage that adversely affect business operations. It describes the processes and procedures an organization establishes to ensure that essential functions can continue during and after a disaster. Business continuity prevents interruption of mission-critical services, and reestablishes the impacted services as swiftly and smoothly as possible by using an automated process. BC involves proactive measures such as business impact analysis, risk assessment, building resilient IT infrastructure, deploying data protection solutions (backup and replication). It also involves reactive countermeasures such as disaster recovery (discussed later in this module). In a software-defined data center, policy-based services can be created that include data protection through the self-service portal. Consumers can select the class of service that best meets their performance, cost, and protection requirements on demand. Once the service is activated, the underlying data protection solutions required to support the service is automatically invoked to meet the required data protection. For example if a service requires VM backup for every six hours, then backing up VM is scheduled automatically every six hours. The goal of a BC solution is to ensure “information availability” required to conduct vital business operations.

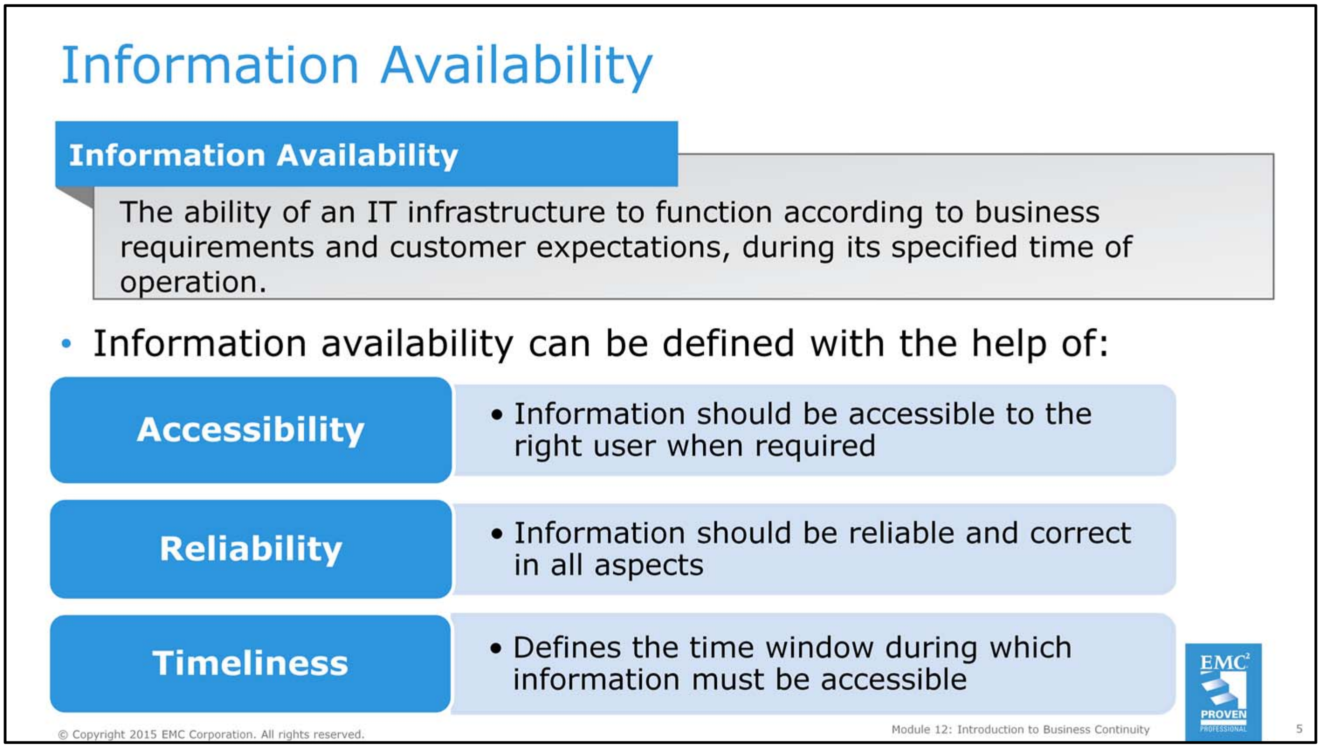


Why Business Continuity?

- Continuous access to information ensures smooth functioning of business operations
  - Generates revenue, productivity is not impacted, and reputation is maintained
- Organizations must ensure that demanding SLAs are met
  - Cost of unavailability of information to an organization is greater than ever
- There are many threats to business continuity
- It is critical for businesses to have appropriate process in place to overcome the challenges

Today, businesses rely on information more than ever. Continuous access to information is a must for the smooth functioning of business operations for any organization. The organizations are under pressure to deliver services to customers in accordance with service level agreements (SLAs). The cost of unavailability of information is greater than ever, and outages in key industries cost millions of dollars per hour. There are also compliance issues, especially if an organization holds consumer data. The failure to meet industry or government regulations may result in hefty fines; and loss of business-critical data could compound the financial impact significantly.

There are many threats to business continuity, such as natural disasters, unplanned occurrences, and planned occurrences that could result in the inaccessibility of information. IT organizations are increasingly embracing bring-your-own-device (BYOD) to improve their employee productivity, lower costs, and support flexible working conditions. However, they also bring potential risks if they are not deployed smartly due to the fact that the business data (sensitive and critical data) may also be stored on these devices. Therefore, it is critical for businesses to define appropriate strategies that can help them to overcome these crises in order to provide continuous access to information. Business continuity is an important process to define and implement these strategies.



Information Availability

Information Availability

The ability of an IT infrastructure to function according to business requirements and customer expectations, during its specified time of operation.

- Information availability can be defined with the help of:

Accessibility
- Information should be accessible to the right user when required

Reliability
- Information should be reliable and correct in all aspects

Timeliness
- Defines the time window during which information must be accessible

© Copyright 2015 EMC Corporation. All rights reserved.

Module 12: Introduction to Business Continuity

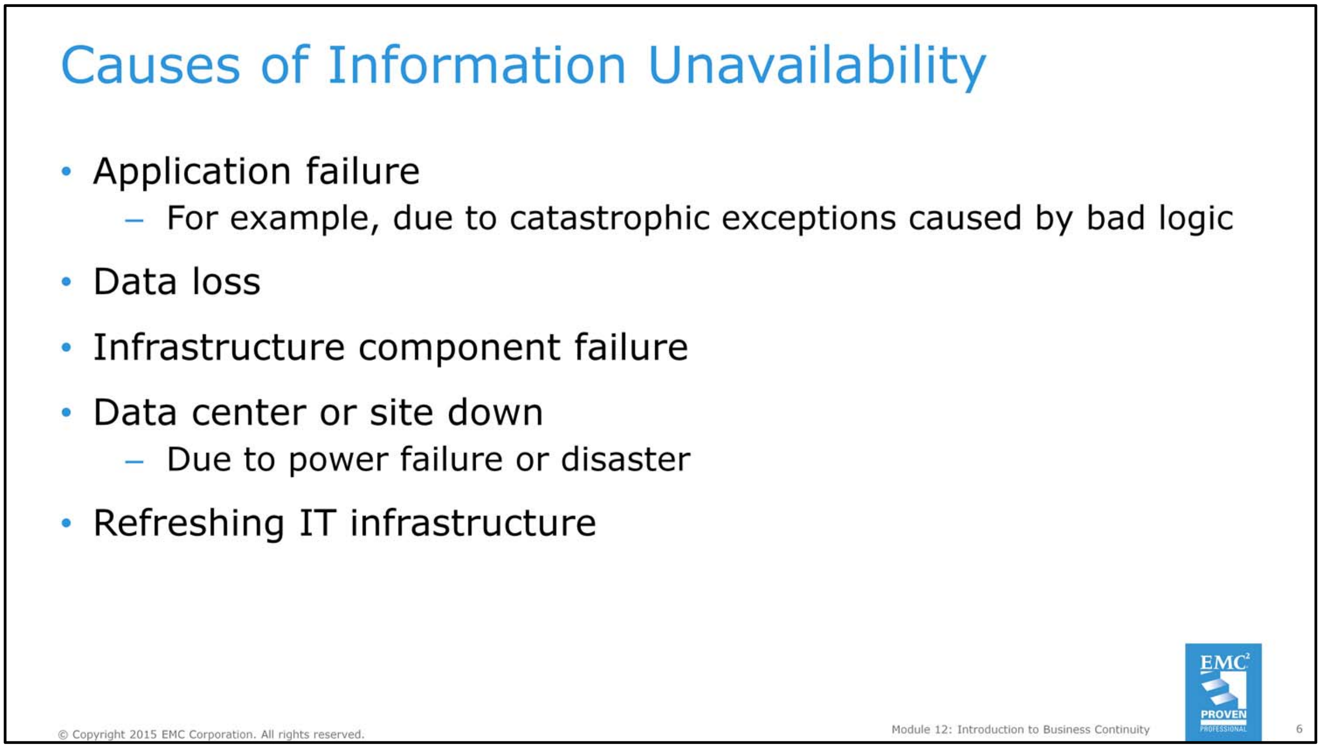
5

Information availability (IA) refers to the ability of an IT infrastructure to function according to business requirements and customer expectations during its specified time of operation. IA ensures that people (employees, customers, suppliers, and partners) can access information whenever they need it. IT organizations need to design and build their infrastructure to maximize the availability of the information, while minimizing the impact of an outage on consumers. IA can be defined in terms of accessibility, reliability, and timeliness of information.

Accessibility: Information should be accessible to the right user when required.

Reliability: Information should be reliable and correct in all aspects. It is “the same” as what was stored and there is no alternation or corruption to the information.

Timeliness: Defines the time window (a particular time of the day, week, month, and year as specified) during which information must be accessible. For example, if online access to an application is required between 8:00 am and 10:00 pm each day, any disruption to data availability outside of this time slot is not considered to affect timeliness.



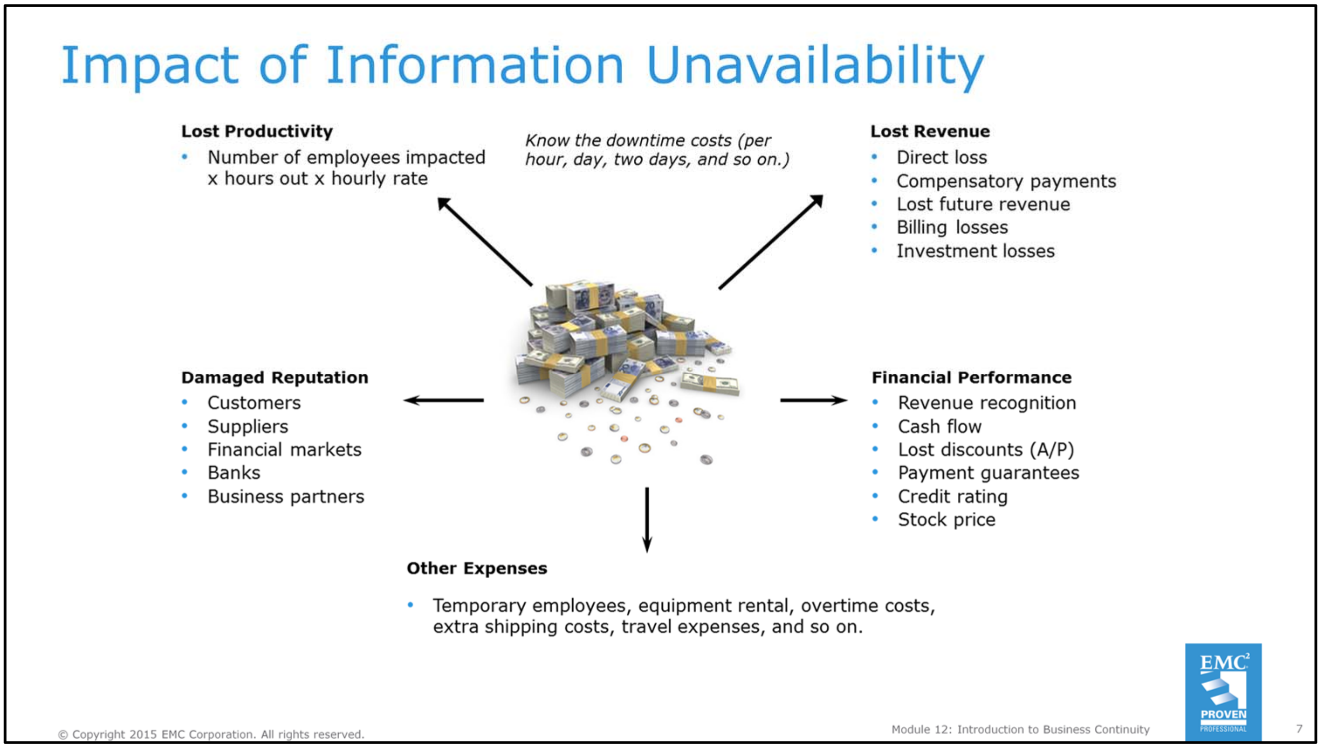
Causes of Information Unavailability

- Application failure
  - For example, due to catastrophic exceptions caused by bad logic
- Data loss
- Infrastructure component failure
- Data center or site down
  - Due to power failure or disaster
- Refreshing IT infrastructure

The slide lists some of the key causes of information unavailability. Data center failure due to disaster (natural or man-made disasters such as flood, fire, earthquake, and so on) is not the only cause of information unavailability. Poor application design or resource configuration errors can also lead to information unavailability. For example, if the database server is down for some reason, then the data is inaccessible to the consumers, which leads to IT service outage. Even the unavailability of data due to several factors (data corruption and human error) leads to outage. The IT department is routinely required to take on activities such as refreshing the data center infrastructure, migration, running routine maintenance, or even relocating to a new data center. Any of these activities can have its own significant and negative impact on information availability.

Note:

In general, the outages can be broadly categorized into planned and unplanned outages. Planned outages may include installation and maintenance of new hardware, software upgrades or patches, performing application and data restores, facility operations (renovation and construction), and migration. Unplanned outages include failure caused by human errors, database corruption, failure of physical and virtual components, and natural or human-made disasters.



Impact of Information Unavailability

Lost Productivity

- Number of employees impacted x hours out x hourly rate

Know the downtime costs (per hour, day, two days, and so on.)

Lost Revenue

- Direct loss
- Compensatory payments
- Lost future revenue
- Billing losses
- Investment losses

Damaged Reputation

- Customers
- Suppliers
- Financial markets
- Banks
- Business partners

Financial Performance

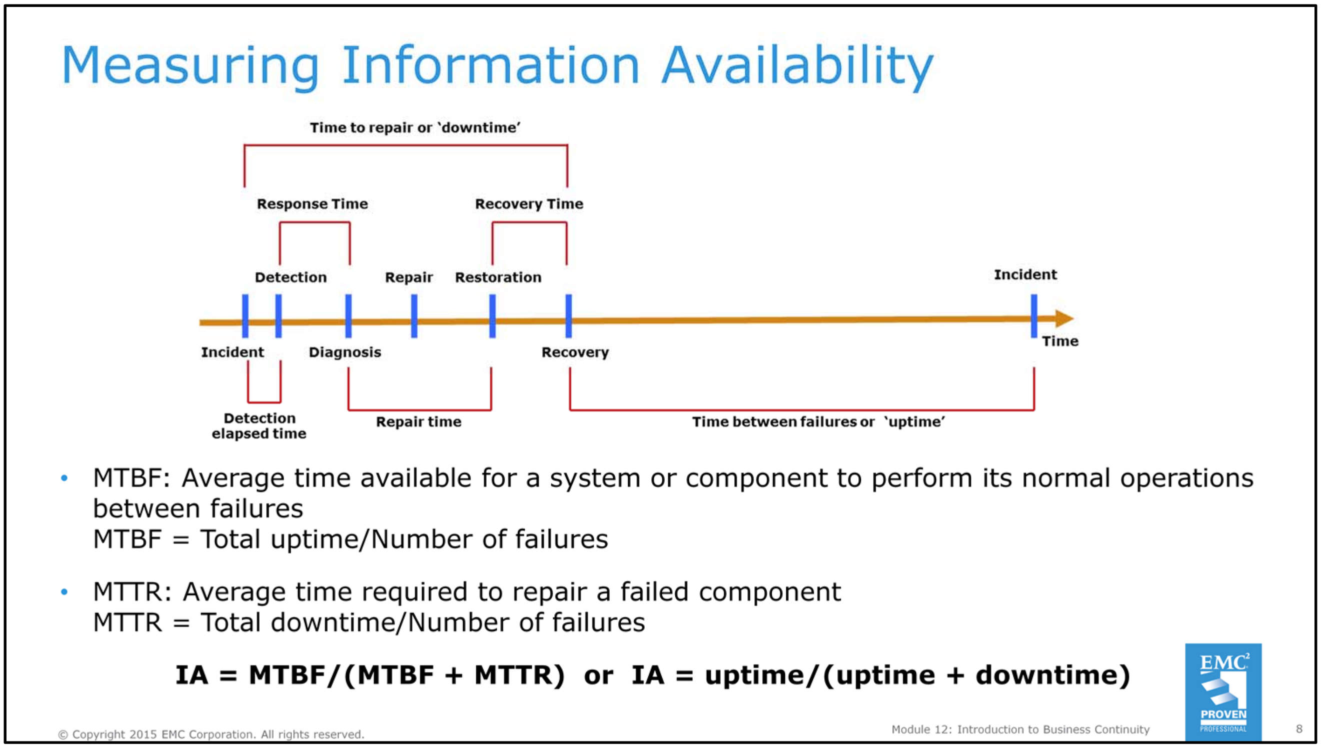
- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees
- Credit rating
- Stock price

Other Expenses

- Temporary employees, equipment rental, overtime costs, extra shipping costs, travel expenses, and so on.

Module 12: Introduction to Business Continuity 7

IT service outage, due to information unavailability, results in loss of productivity, loss of revenue, poor financial performance, and damages to reputation. The loss of revenue includes direct loss, compensatory payments, future revenue loss, billing loss, and investment loss. The damages to reputations may result in a loss of confidence or credibility with customers, suppliers, financial markets, banks, and business partners. The other possible consequences of outage include the cost of additional rented equipment, overtime, and extra shipping.



Measuring Information Availability

- MTBF: Average time available for a system or component to perform its normal operations between failures
  MTBF = Total uptime/Number of failures
- MTTR: Average time required to repair a failed component
  MTTR = Total downtime/Number of failures

IA = MTBF/(MTBF + MTTR) or IA = uptime/(uptime + downtime)

Information availability relies on the availability of both physical and virtual components of a data center. The failure of these components might disrupt information availability. A failure is the termination of a component's ability to perform a required function. The component's ability can be restored by performing various external corrective actions, such as a manual reboot, a repair, or replacement of the failed component(s). Proactive risk analysis, performed as part of the BC planning process, considers the component failure rate and average repair time, which are measured by MTBF and MTTR:

Mean Time Between Failure (MTBF): It is the average time available for a system or component to perform its normal operations between failures. It is the measure of system or component reliability and is usually expressed in hours.

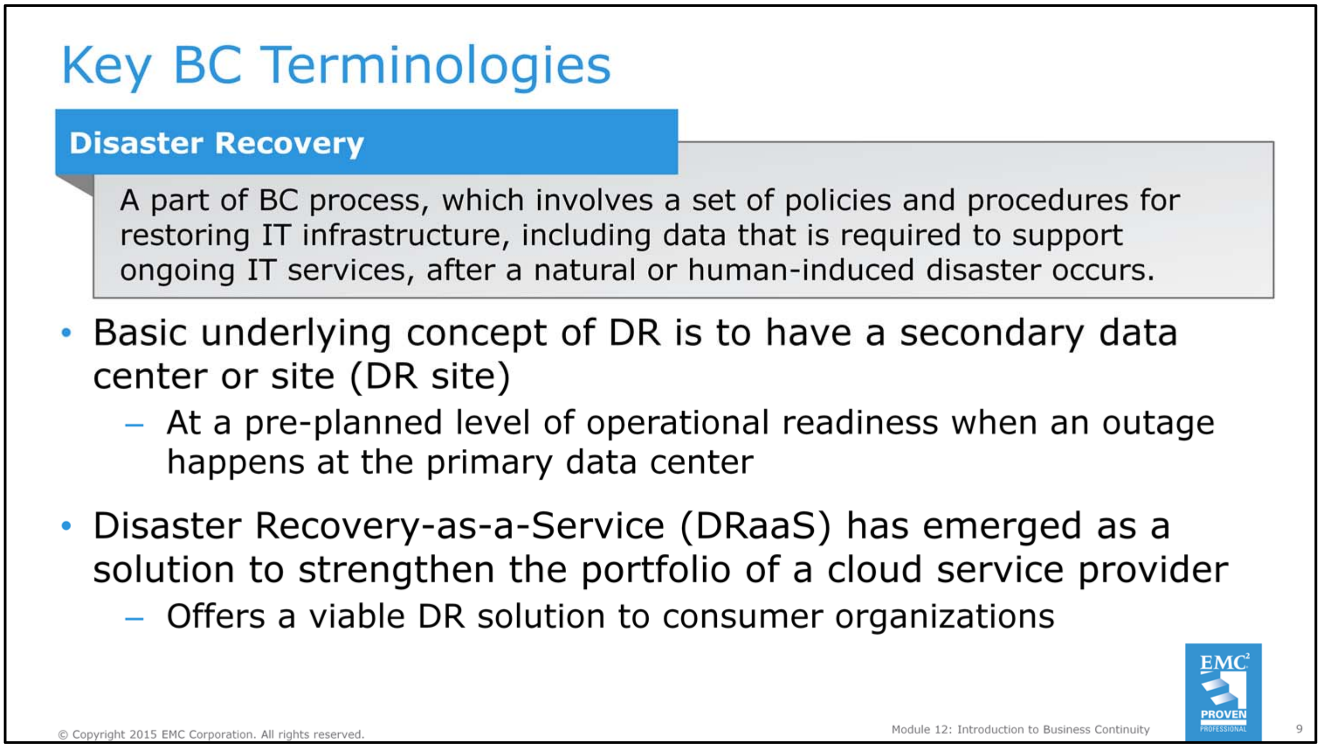
Mean Time To Repair (MTTR): It is the average time required to repair a failed component. MTTR includes the total time required to do the following activities: detect the fault, mobilize the maintenance team, diagnose the fault, obtain the spare parts, repair, test, and restore the data.

IA can be expressed in terms of system uptime and downtime and measured as the amount or percentage of system uptime:

IA = system uptime/(system uptime + system downtime), where system uptime is the period of time during which the system is in an accessible state; when it is not accessible, it is termed as system downtime. In terms of MTBF and MTTR, IA could also be expressed as: IA = MTBF/(MTBF + MTTR)

Note:

Uptime per year is based on the exact timeliness requirements of the service. This calculation leads to the number of "9s" representation for availability metrics. For example, a service that is said to be "five 9s available" is available for 99.999 percent of the scheduled time in a year (24×365).



Key BC Terminologies

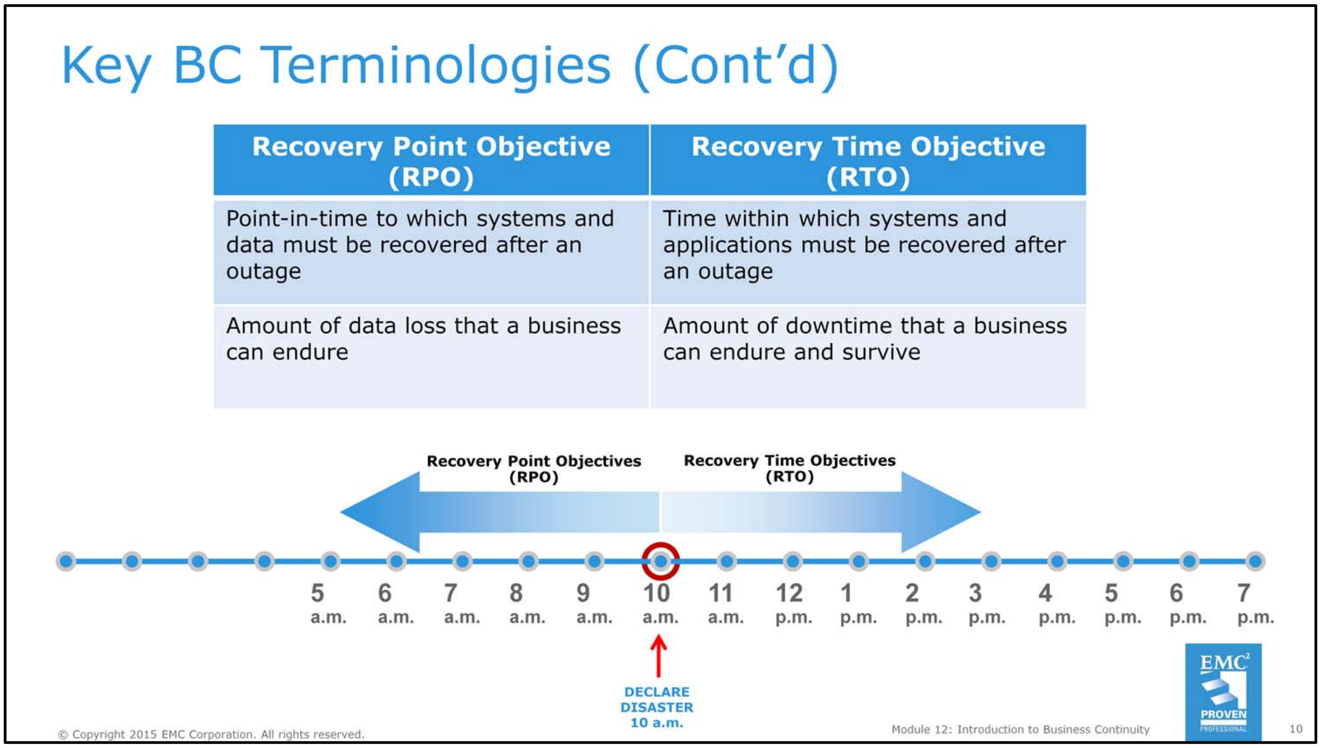
Disaster Recovery

A part of BC process, which involves a set of policies and procedures for restoring IT infrastructure, including data that is required to support ongoing IT services, after a natural or human-induced disaster occurs.

- Basic underlying concept of DR is to have a secondary data center or site (DR site)
  - At a pre-planned level of operational readiness when an outage happens at the primary data center
- Disaster Recovery-as-a-Service (DRaaS) has emerged as a solution to strengthen the portfolio of a cloud service provider
  - Offers a viable DR solution to consumer organizations

Disaster recovery (DR) is a part of BC process which involves a set of policies and procedures for restoring IT infrastructure, including data that is required to support the ongoing IT services, after a natural or human-induced disaster occurs. Disaster Recovery Plans (DRP) are generally part of a larger, more extensive practice known as Business Continuity Planning. DR plans should be well practiced so that the key people become familiar with the specific actions they will need to take when a disaster occurs. DR plans must also be adaptable and routinely updated, e.g. if some new people, a new branch office, or some new hardware or software are added to an organization, they should promptly be incorporated into the organization's disaster recovery plan. The companies must consider all these facets of their organization as well as update and practice their plan if they want to maximize their recovery after a disaster. The basic underlying concept of DR is to have a secondary data center or site (DR site) and at a pre-planned level of operational readiness when an outage happens at the primary data center. Typically in a DR process, a previous copy of the data is restored and logs are applied to that copy to bring it to a known point of consistency. After all recovery efforts are completed, the data is validated to ensure that it is correct.

The disaster recovery methods often require buying and maintaining a complete set of IT resources at secondary data centers that matches the business-critical systems at the primary data center. This includes sufficient storage to house a complete copy of all of the enterprise’s business data by regularly copying production data on the mirror systems at secondary site. This may be a complex process and expensive solution for a significant number of organizations. Disaster Recovery-as-a-Service (DRaaS) has emerged as a solution to strengthen the portfolio of a cloud service provider, while offering a viable DR solution to consumer organizations. Having DR sites in the cloud reduces the need for data center space, IT infrastructure, and IT resources, which lead to significant cost reductions to organizations. DRaaS is further discussed in module 14, ‘Replication’.



Key BC Terminologies (Cont'd)

Recovery Point Objective (RPO)	Recovery Time Objective (RTO)
Point-in-time to which systems and data must be recovered after an outage	Time within which systems and applications must be recovered after an outage
Amount of data loss that a business can endure	Amount of downtime that a business can endure and survive

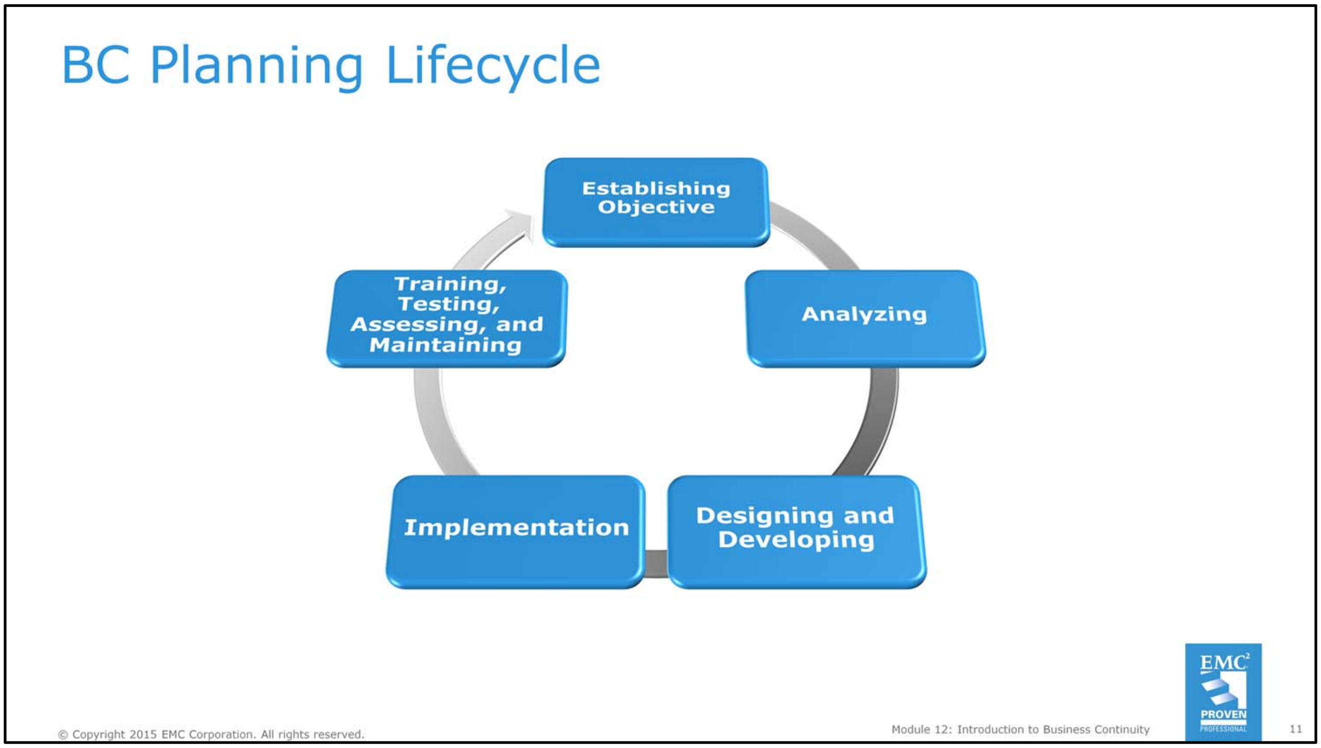
Module 12: Introduction to Business Continuity 10

As more critical applications are virtualized and data centers move towards software-defined approach, it is important for organizations to know that not all applications have the same recovery requirements. When designing a business continuity strategy, businesses must consider the two important parameters that are closely associated with recovery.

Recovery Point Objective (RPO): This is the point-in-time to which systems and data must be recovered after an outage. It defines the amount of data loss that a business can endure. Based on the RPO, organizations plan for the frequency with which a backup or replica must be made. An organization can plan for an appropriate BC technology solution on the basis of the RPO it sets. For example, if the RPO of a particular business application is 24 hours, then backups are created every midnight. The corresponding recovery strategy is to restore data from the set of last backup.

Recovery Time Objective (RTO): This is the time within which systems and applications must be recovered after an outage. It defines the amount of downtime that a business can endure and survive. For example, if the RTO is a few seconds, then implementing global clustering would help to achieve the required RTO. The more critical the application, the lower the RTO should be.

Both RPO and RTO are counted in minutes, hours, or days and are directly related to the criticality of the IT service and data. The lower the number of RTO and RPO, the higher will be the cost of a BC solution.



BC Planning Lifecycle

Establishing Objective

Analyzing

Designing and Developing

Implementation

Training, Testing, Assessing, and Maintaining

© Copyright 2015 EMC Corporation. All rights reserved.

Module 12: Introduction to Business Continuity

11

BC planning must follow a disciplined approach like any other planning process. Organizations today dedicate specialized resources to develop and maintain BC plans. From the conceptualization to the realization of the BC plan, a lifecycle of activities can be defined for the BC process. The BC planning lifecycle includes five stages:

1. Establishing objectives

- Determine BC requirements

- Estimate the scope and budget to achieve requirements

- Select a BC team that includes subject matter experts from all areas of business, whether internal or external

- Create BC policies

2. Analyzing

- Collect information on data profiles, business processes, infrastructure support, dependencies, and frequency of using business infrastructure

- Conduct a business impact analysis

- Identify critical business processes and assign recovery priorities

- Perform risk analysis for critical functions and create mitigation strategies

- Perform cost benefit analysis for available solutions based on the mitigation strategy

- Evaluate options

(Cont’d)

3. Designing and developing

- Define the team structure and assign individual roles and responsibilities; for example, different teams are formed for activities such as emergency response and infrastructure and application recovery

- Design data protection strategies and develop infrastructure

- Develop contingency solution and emergency response procedures

- Detail recovery and restart procedures

4. Implementing

- Implement risk management and mitigation procedures that include backup, replication, and management of resources

- Prepare the DR sites that can be utilized if a disaster affects the primary data center. The DR site could be one of the organization’s own data center or could be a cloud

- Implement redundancy for every resource in a data center to avoid single points of failure

5. Training, testing, assessing, and maintaining

- Train the employees who are responsible for backup and replication of business-critical data on a regular basis or whenever there is a modification in the BC plan

- Train employees on emergency response procedures when disasters are declared

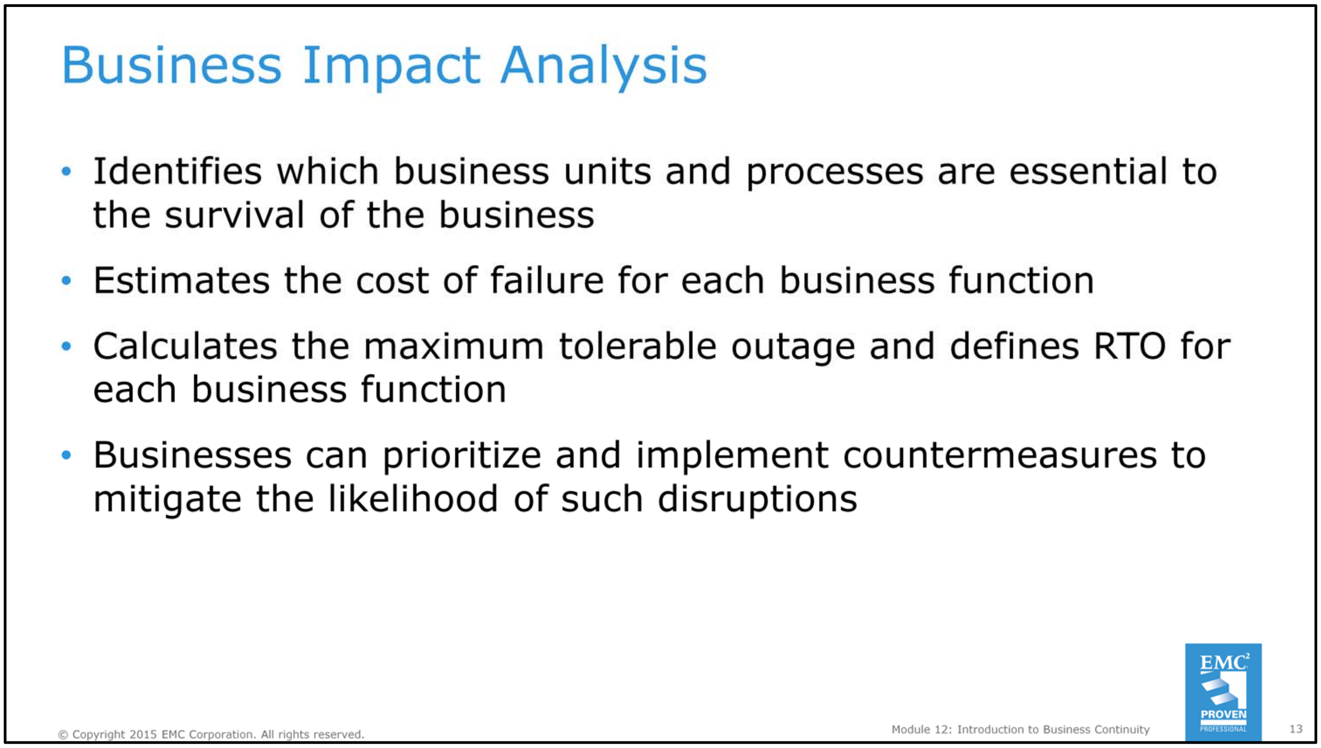
- Train the recovery team on recovery procedures based on contingency scenarios

- Perform damage-assessment processes and review recovery plans

- Test the BC plan regularly to evaluate its performance and identify its limitations

- Assess the performance reports and identify limitations

- Update the BC plans and recovery/restart procedures to reflect regular changes within the data center



Business Impact Analysis

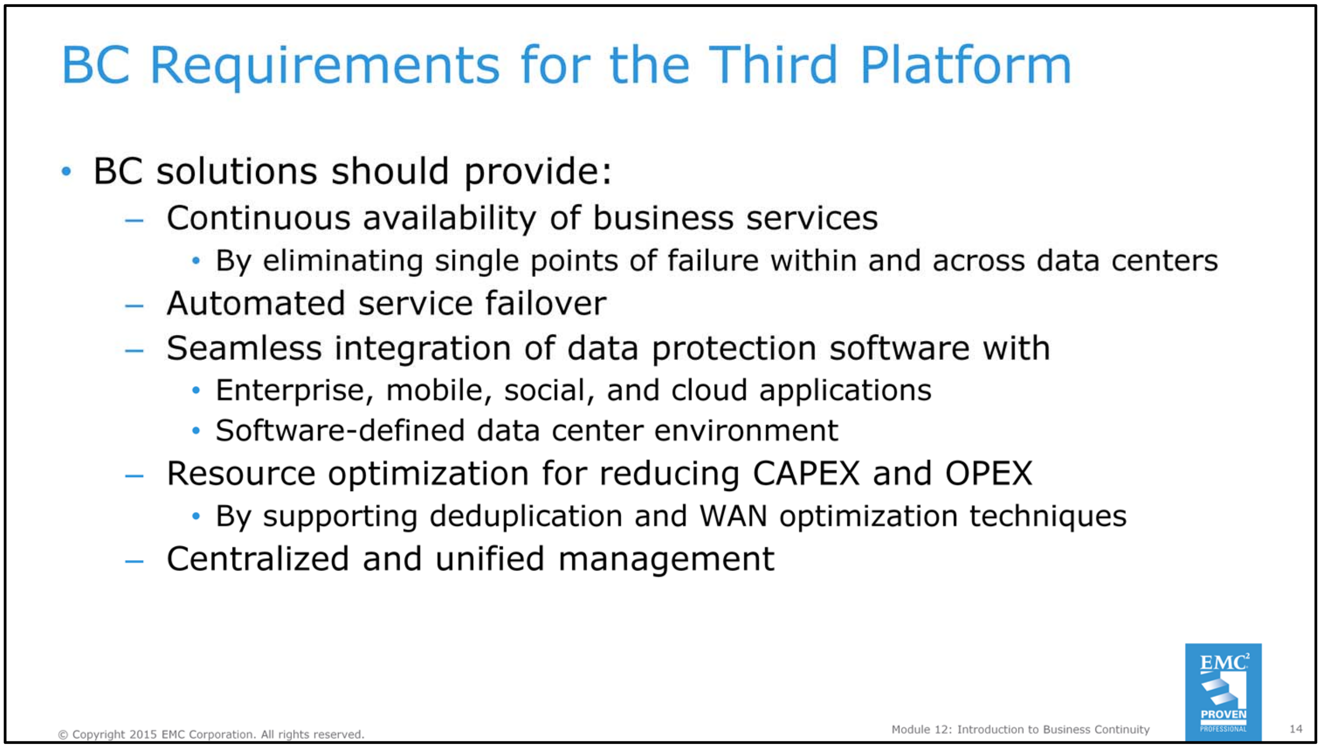
- Identifies which business units and processes are essential to the survival of the business
- Estimates the cost of failure for each business function
- Calculates the maximum tolerable outage and defines RTO for each business function
- Businesses can prioritize and implement countermeasures to mitigate the likelihood of such disruptions

© Copyright 2015 EMC Corporation. All rights reserved.

Module 12: Introduction to Business Continuity 13

A *business impact analysis* (BIA) identifies which business units, operations, and processes are essential to the survival of the business. It evaluates the financial, operational, and service impact of a disruption to essential business processes. The selected functional areas are evaluated to determine resilience of the infrastructure to support information availability. The BIA process leads to a report detailing the incidents and their impact over business functions. The impact may be specified in terms of money or in terms of time. Based on the potential impact associated with downtime, businesses can prioritize and implement countermeasures to mitigate the likelihood of such disruptions. These are detailed in the BC plan. A BIA includes the following set of tasks:

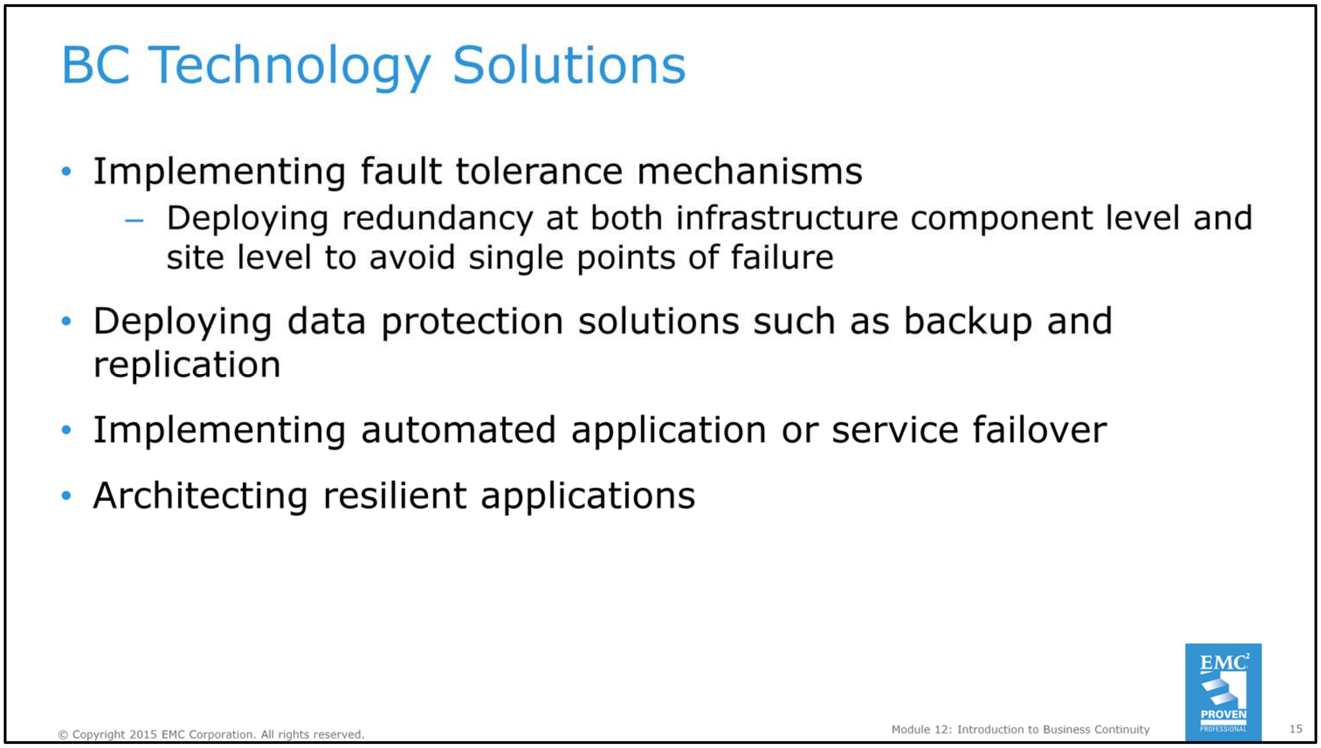
- Determine the business areas.
- For each business area, identify the key business processes critical to its operation.
- Determine the attributes of the business process in terms of applications, databases, and hardware and software requirements.
- Estimate the costs of failure for each business process.
- Calculate the maximum tolerable outage and define RTO for each business process.
- Establish the minimum resources required for the operation of business processes.
- Determine the recovery strategies and the cost of implementing them.
- Optimize the business recovery strategy based on business priorities.
- Analyze the current state of BC readiness and optimize the future BC planning.



BC Requirements for the Third Platform

- BC solutions should provide:
  - Continuous availability of business services
    - By eliminating single points of failure within and across data centers
  - Automated service failover
  - Seamless integration of data protection software with
    - Enterprise, mobile, social, and cloud applications
    - Software-defined data center environment
  - Resource optimization for reducing CAPEX and OPEX
    - By supporting deduplication and WAN optimization techniques
  - Centralized and unified management

The rise of the third platform has reached a tipping point according to IDC, and with the growth of investments in the cloud, big data, mobile, and social computing, there is, in effect, no way of avoiding it by any organizations. Applications that support these technologies require significantly higher performance, scalability, and availability compared to the traditional applications. It has become increasingly important for IT organizations to deliver services to their customers in accordance with the SLAs. Business continuity solutions must also be ready to support the requirements of third platform applications. The slide provides a list of key BC requirements.



BC Technology Solutions

- Implementing fault tolerance mechanisms
  - Deploying redundancy at both infrastructure component level and site level to avoid single points of failure
- Deploying data protection solutions such as backup and replication
- Implementing automated application or service failover
- Architecting resilient applications

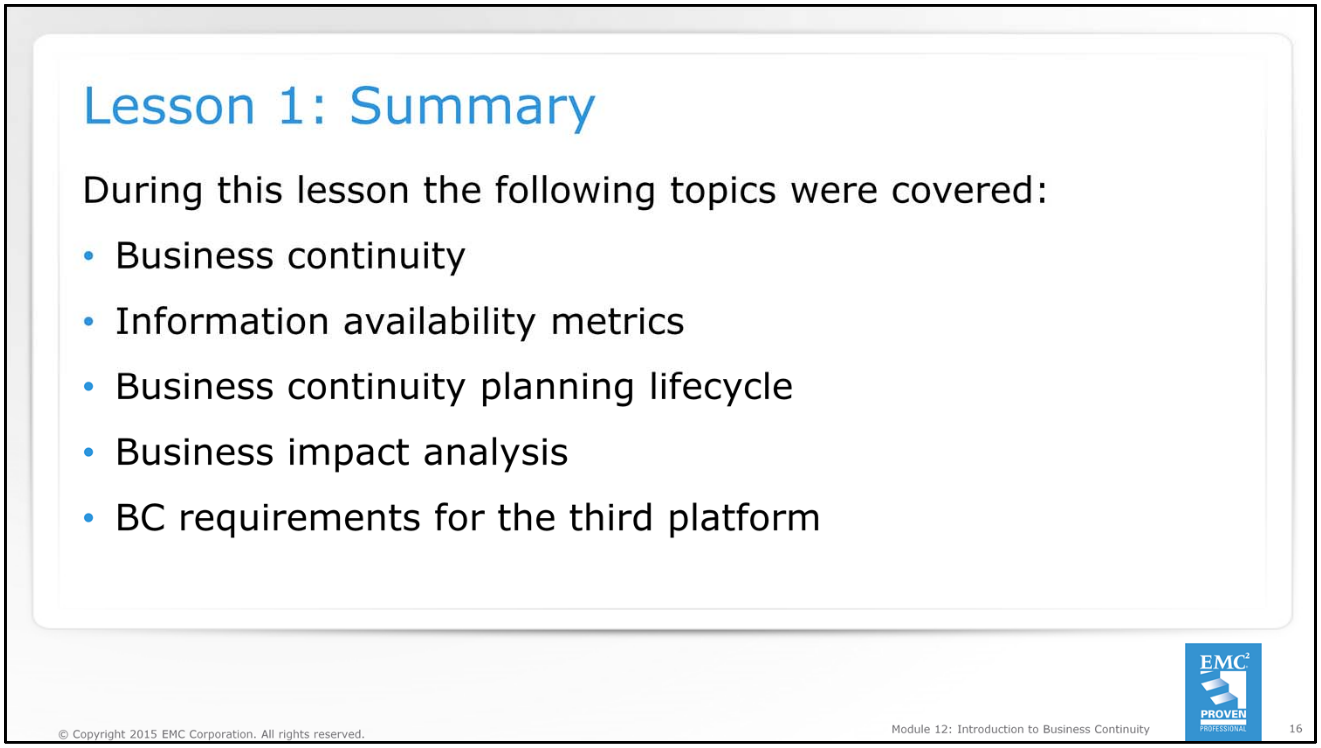
© Copyright 2015 EMC Corporation. All rights reserved.

Module 12: Introduction to Business Continuity 15

With the aim of meeting the required availability, organizations should build a resilient IT infrastructure. Building a resilient IT infrastructure requires the following high availability solutions:

- Deploying redundancy at both the component level and the site (data center) level to avoid single points of failure
- Deploying data protection solutions such as backup and replication
- Implementing automated application failover
- Architecting resilient applications

For example, as soon as a disaster occurs, the BC solution automatically triggers the DR process. This process typically involves both operational personnel and automated procedure in order to reactivate the service (application) at a functioning data center. This requires the transfer of application users, data, and services to the new data center. This involves the use of redundant infrastructure across different geographic locations, live migration, backup, and replication solutions.



Lesson 1: Summary

During this lesson the following topics were covered:

- Business continuity
- Information availability metrics
- Business continuity planning lifecycle
- Business impact analysis
- BC requirements for the third platform

This lesson covered the importance of business continuity solutions to an organization, factors that can affect information availability, and the consequences of information unavailability. This lesson covered information availability metrics namely mean time between failure (MTBF) and mean time to repair (MTTR). Further this lesson covered business continuity planning lifecycle and business impact analysis. Finally, this lesson covered the BC requirements for third platform.