# Business Continuity and Disaster Recovery

Week 6 – Business Impact Analysis (BIA)

# Week 6: CHAPTER 5 Outline

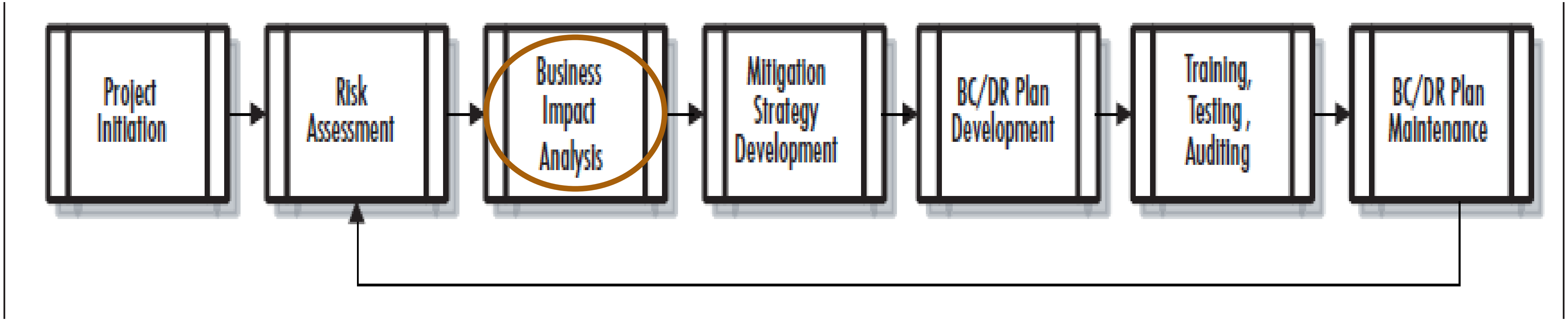
## RECAP FROM WEEK 5

- Risk management basics
- People, Process, Technology and Infrastructure in Risk Management
- IT Specific Risk Management
- Risk assessment components
- Threat assessment methodology
- Vulnerability assessment

## WEEK 6

- Business impact analysis overview
- Understanding impact criticality
- Identifying business functions and processes
- Gathering data for the business impact analysis
- Determining the impact
- Business impact analysis data points
- Preparing the business impact analysis report

# Basic Steps in BCDR Plan



# Introduction: Risk Management vs. BIA (Snedaker & Rima, 2014)

Business impact analysis (BIA) looks at

- the critical business functions
- the impact of not having those functions available to the firm
- the impact of various business functions on your operations

RA & BIA are both organizational assessments, but

- The risk assessment starts from the threat side
- The business impact analysis starts from the business process side

Outputs from both, are used as input to the mitigation strategy development

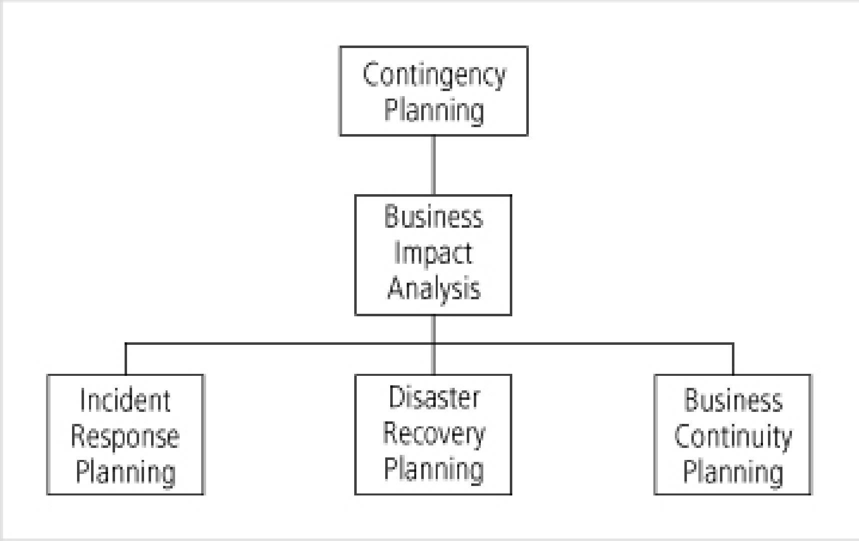
# Introduction: Risk Management vs. BIA
(Whitman & Mattord, 2019)

The business impact analysis (BIA)

- the first phase of the CP process and serves as an investigation and assessment of the impact that various adverse events can have on the organization

Fundamental differences between a BIA and risk management

- Risk management focuses on identifying the threats, vulnerabilities, and attacks to determine which controls can protect the information
- The BIA assumes that
  - controls have been bypassed, have failed, or have otherwise proved ineffective,
  - the attack succeeded, and that the adversity that was being defended against has been successful


Contingency Planning
Business Impact Analysis
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning

BIA provides guidance toward the creation of the IR, DR, and BC plans

# Business Impact Analysis Overview
(Snedaker & Rima, 2014)

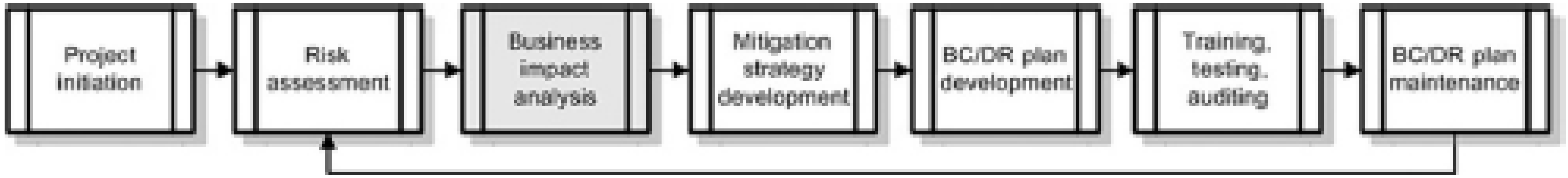
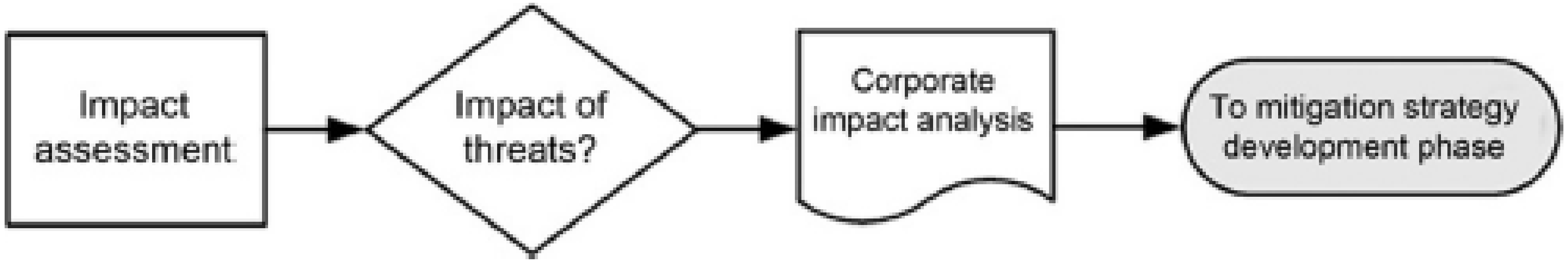


**FIGURE 5.1**

Business continuity and disaster recovery project progress.



Impact assessment
Impact of threats?
Corporate impact analysis
To mitigation strategy development phase

**FIGURE 5.2**

Business impact analysis phase.

# BUSINESS IMPACT ANALYSIS OVERVIEW

# Business Impact Analysis Overview
(Snedaker & Rima, 2014)

The fundamental task in the BIA is to understand which processes in your business are vital to your ongoing operations and to understand the impact the disruption of these processes would have on your business.

From an IT perspective, NIST views BIA as “Its purpose is to correlate specific **system components** with the **critical services** that they provide, and based on that information, to characterize the consequences of a disruption to the system components.” (Source: NIST Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34,p.16).

There are two parts to the BIA:

- to understand mission-critical business processes
- to correlate those to IT systems.

# Business Impact Analysis Overview
## (Snedaker & Rima, 2014)

As an IT professional,

- you certainly understand the importance of various IT systems, but
- you may not be fully aware of the critical business functions performed in your company.

understanding the critical business functions is important to recover IT systems in the event of a significant business disruption.

Four primary purposes of BIA (Business Continuity Institute, 2013):

1. Obtain an understanding of the organization’s **most critical objectives**, the priority of each, and the timeframe for resumption of these following an unscheduled interruption.
2. **Inform a management decision on Maximum Tolerable Outage (MTO)** for each function.
3. **Provide the resource information** from which an appropriate recovery strategy can be determined/recommended.
4. **Outline dependencies that exist both internally and externally** to achieve critical objectives.

# Business Impact Analysis Overview (Whitman & Mattord, 2019)

The BIA begins with

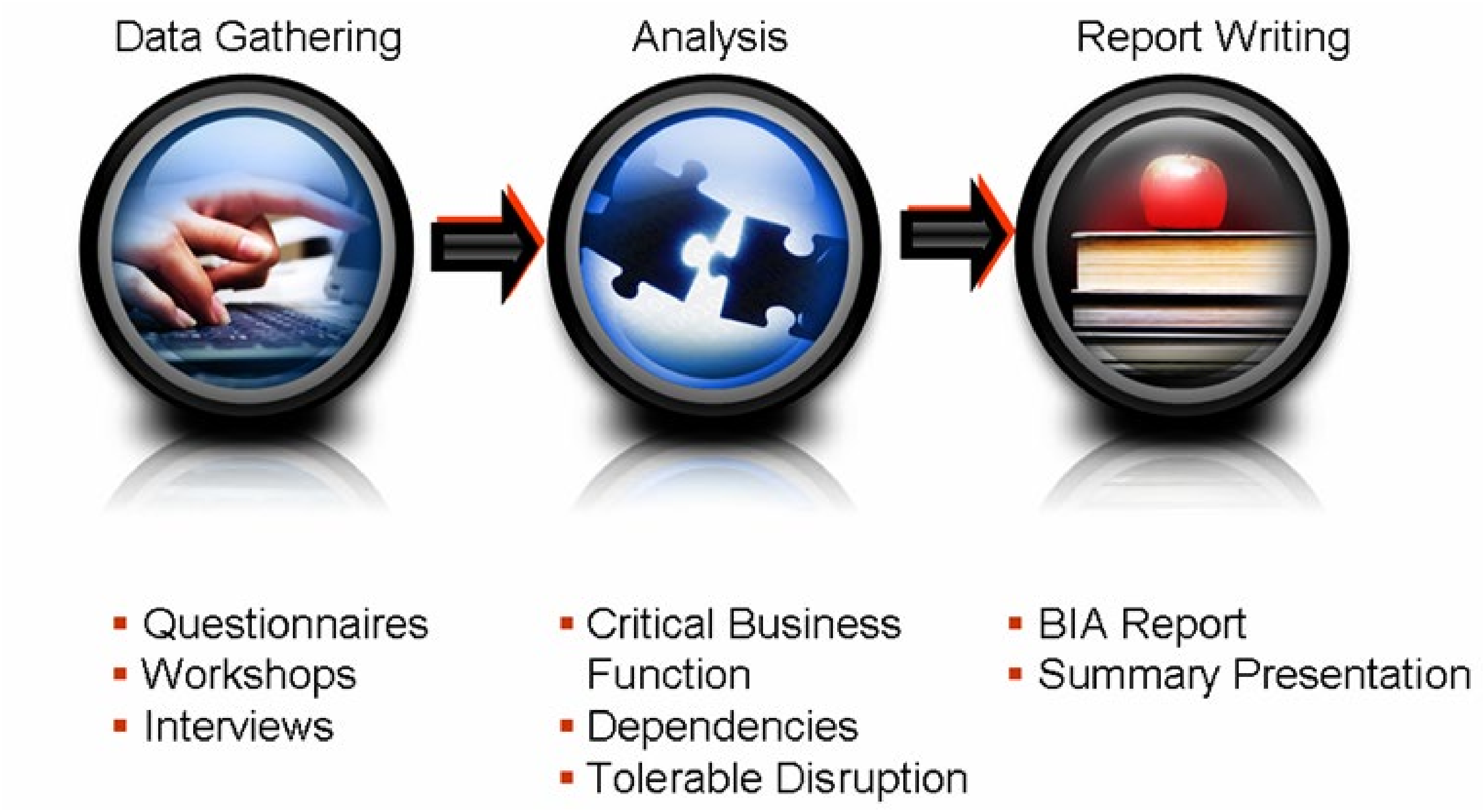
- the prioritized list of threats and vulnerabilities identified in the risk management process, and
- enhances the list by adding the information needed to respond to the adversity

When undertaking the BIA, the organization should consider:

- Scope
- Plan
- Balance
- Objective
- Follow-up

# BIA OVERVIEW FROM THE INDUSTRY

## (BKI PROFESSIONAL SERVICES SDN BHD, 2022)



Data Gathering

- Questionnaires
- Workshops
- Interviews

Analysis

- Critical Business Function
- Dependencies
- Tolerable Disruption

Report Writing

- BIA Report
- Summary Presentation

# BIA STEPS

(SNEDAKER & RIMA, 2014)

1 Identify key business processes and functions.

2 Establish requirements for business recovery.

3 Determine resource interdependencies.

4 Determine impact on operations.

5 Develop priorities and classification of business processes and functions.

6 Develop recovery time requirements.

7 Determine financial, operational, and legal impact of disruption.

The result of performing these seven steps is a formal BIA, which is used in conjunction with the risk assessment analysis to develop mitigation strategies (discussed in Chapter 6).

# Primary Impacts

The two primary impact of any business disruption are

- **the operational impact**: addresses the nonmonetary impact including how **people, processes, and technology** are impacted by a business disruption and how best to address that impact.
- **the financial impact**: addresses the monetary impacts and how a business disruption will impact the **company's revenues**.

Examples of operational impact

- Reduced service levels or output
- Inability to meet key deadlines and deliverables
- Disruption to ongoing projects and/or processes

Examples of financial impact

- Loss of revenue and income
- Cost to recover from a disaster (Lost equipment, materials, and supplies)
- Contractual or regulatory fines and penalties
- Potential lawsuits

# Indirect Impacts (1 of 2)

Indirect impact:

- **Upstream losses**: those you will suffer if one of your key **suppliers** is affected by a disaster
- **Downstream losses**: occur when key **customers** or the lives in your community are affected

Examples of upstream losses

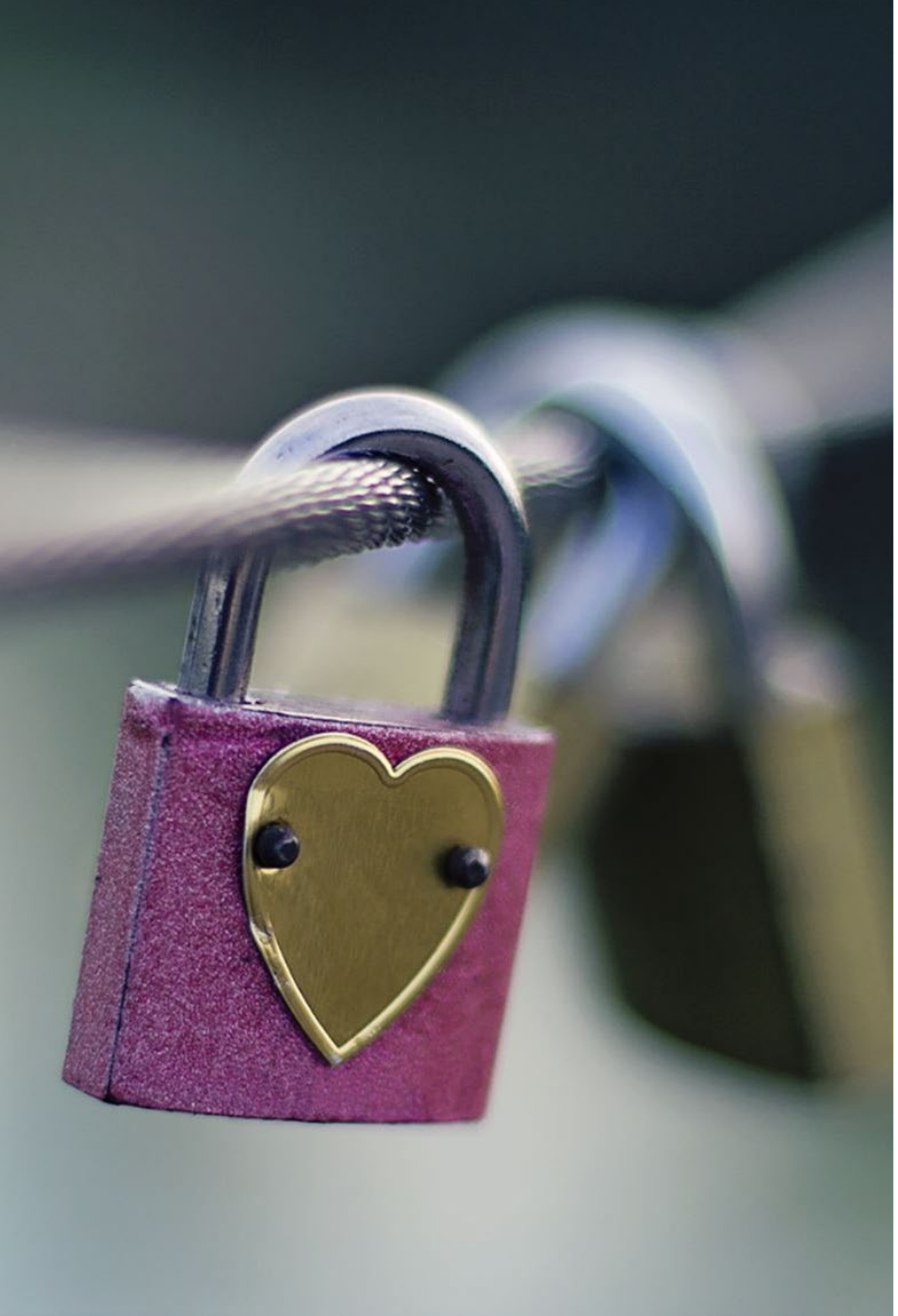
- If your company relies on regular deliveries of products or services by another company, you could experience upstream losses if that company cannot deliver.
- If you run a manufacturing company that relies on raw materials arriving on a set or regular schedule, any disruption to that schedule will impact your company's ability to make and sell its products.
- ***This is how a disaster elsewhere can impact you, even if your company is unharmed***.

# Indirect Impacts (2 of 2)

Examples of downstream losses

- If your business supplies parts to a major manufacturer that is shut down due to a hurricane or earthquake, your sales will certainly suffer.
- if your company provides any type of noncritical service to your community and there is a flood or landslide, your sales could take a hit while residents of the community deal with the disaster.
- If you operate a chain of restaurants or movie theaters or golf courses, residents will be more focused on dealing with the disaster than on entertainment and leisure pursuits.
- ***These are considered downstream losses even if your business, itself, has not taken the direct impact of a disaster.***

People, business, and communities are interrelated. A natural disaster or serious disruption can create a chain reaction that ripples through the business community and impacts the local or regional economy.



# Understanding the Human Impact (1 of 2)

If a natural disaster strikes, it’s possible that some or all of your company’s employees will be impacted

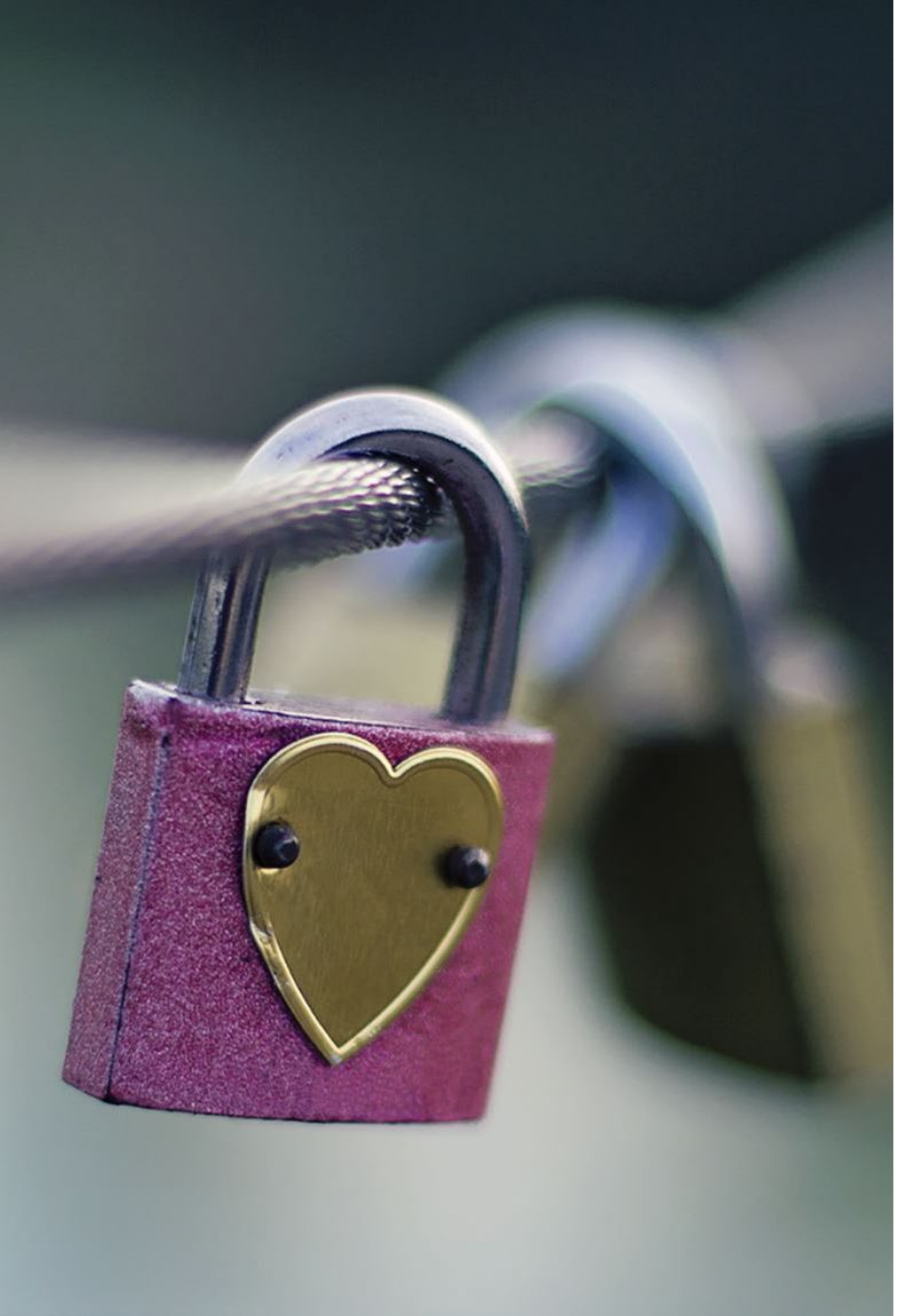
Examples of human impact

- Loss of life and serious injury
- Long-term emotional impact on family, work, and community

Need to identify key positions, key knowledge, and key skills needed for business continuity.

Key positions

- Succession planning - replacing key employees as well as how to transfer the reins of the company from one leader to the next.
- If someone at top level were suddenly unavailable to carry out that function, the business would suffer financial losses.
- address who will replace key employees in the event of a planned or unplanned departure
- the BC/DR plan needs to look at key positions within the company and understand the role of each in the business continuity realm.
- if you have complex database applications, and your DBA is not available, what should you do?



# Understanding the Human Impact (2 of 2)

Human needs

- everyone responds to disasters differently

A good BCP will address the human factors for two reasons

1. addressing employee needs is simply the right thing to do
    - HR comes up with policies to address employees’ needs and requirements in the aftermath (business disruptions or natural disaster)
    - IT systems recovery requires experienced network administrators
2. because it makes good business sense
    - Need to come up with appropriate alternatives that can address the lack of key staff in the aftermath of a business disruption.
    - helps the employees who may be unable to come back immediately and also helps the company recover in the fastest, most efficient manner possible.

# Understanding impact criticality

# Criticality categories

You can develop any category system that works for you but as with all rating systems, be sure the categories are clearly defined and that there is a shared understanding of the proper use and scope of each. Here is one commonly used rating system for assessing criticality:

- Category 1: Critical Functions–Mission-Critical (0-12 hours)
- Category 2: Essential Functions–Vital (13-24 hours)
- Category 3: Necessary Functions–Important (1-3 days)
- Category 4: Desirable Functions–Minor (more than 3 days)

Obviously, your business continuity plan will focus the most time and resources on analyzing the critical functions first, essential functions second.

It’s possible you will delay dealing with necessary and desirable functions until later stages of your business recovery.

# 1. Critical functions—Mission-Critical

Mission-critical business processes and functions are those that have the **greatest impact** on your company’s operations and potential for recovery.

Functions that need to be up and running immediately after disruption

What are the processes that MUST be present for your company to do business?

From an IT perspective, the network, system, or application outage that is mission -critical would cause extreme disruption to the business.

Such an outage often has serious legal and financial issues.

This type of outage may threaten the health, well-being, and safety of individuals

The recovery time: hours, not days

# 2. Essential functions—Vital

Some business functions may fall somewhere between mission-critical an important, so you may choose to use a middle category that is labeled “vital” or “essential.”

Should be addressed immediately after the mission-critical functions.

Vital functions might include things like payroll

Functions that might not be mission-critical but can be vital to the company’s ability to function beyond the disaster recovery stage.

From an IT perspective, vital systems might include those that interface with mission critical systems

The recovery time: hours or a day or two

This category may be eliminated – only focus on mission-critical, important, and minor

# 3. Necessary functions—Important

Important business functions and processes won’t stop the business from operating in the near term but they usually have a longer-term impact if they’re missing or disabled

When missing, these kinds of functions and processes cause some disruption to the business.

They may have some legal or financial ramifications and they may also be related to access across functional units and across business systems.

From an IT perspective, these systems may include e -mail, Internet access, databases, and other business tools that are used in a support function

The recovery time: days or weeks.

# 4. Desirable functions—Minor

Minor business processes are often those that have been developed over time to deal with small, recurring issues or functions.

They ***will not be missed in the near-term*** and certainly not while business operations are being recovered.

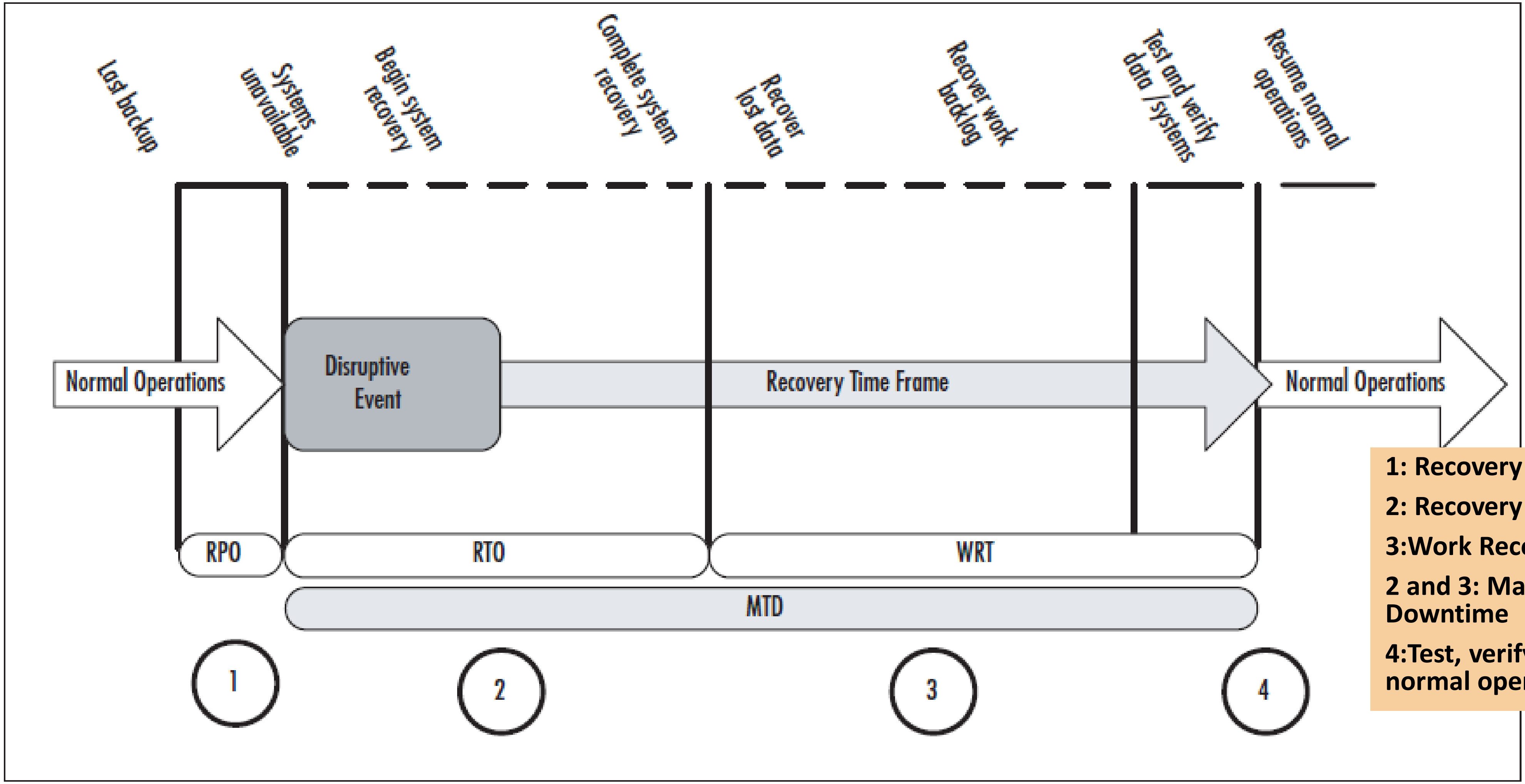
They will need ***to be recovered over the longer-term***.

Some minor business processes may be lost after a significant disruption and in some cases, that's just fine.

From an IT perspective, these types of system outages cause minor disruptions to the business and they can be easily restored.

The recovery time: weeks or months

# Recovery Time Requirements



**1: Recovery Point Objective**

**2: Recovery Time Objective**

**3:Work Recovery Time**

**2 and 3: Maximum Tolerable Downtime**

**4:Test, verify, and resume normal operations**

# Recovery Time Requirements

Point 1: RPO—The maximum sustainable data loss based on backup schedules and data needs.

Point 2: RTO—The duration of time required to bring critical systems back online.

Point 3: WRT—The duration of time needed to recover lost data (based on RPO) and to enter data resulting from work backlogs (manual data generated during system outage that must be entered).

Points 2 and 3: MTD—The duration of the RTO plus the WRT.

Point 4: Test, verify, and resume normal operations.

# Recovery Time Requirements

**Recovery Point Objective (RPO)**

- The amount or extent of data loss that can be tolerated by your critical business systems
- For example, some companies perform real-time data backup, some perform hourly or daily backups, some perform weekly backups.
- If you perform weekly backups, someone made a decision that your company could tolerate the loss of a week's worth of data. The RPO is one week.

**Recovery Time Objective (RTO)**

- The time available to recover disrupted systems and resources (systems recovery time).

# Recovery Time Requirements

## Work Recovery Time (WRT)

- It takes time to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored.
- additional steps that must be undertaken before it’s back to business

## Maximum Tolerable Downtime (MTD)

- the maximum time a business can tolerate the absence or unavailability of a particular business function
- If a business function is categorized as mission-critical (Category 1), it will have the shortest MTD`
- The higher the criticality, the shorter the maximum tolerable downtime

# Identifying business functions

# BIA

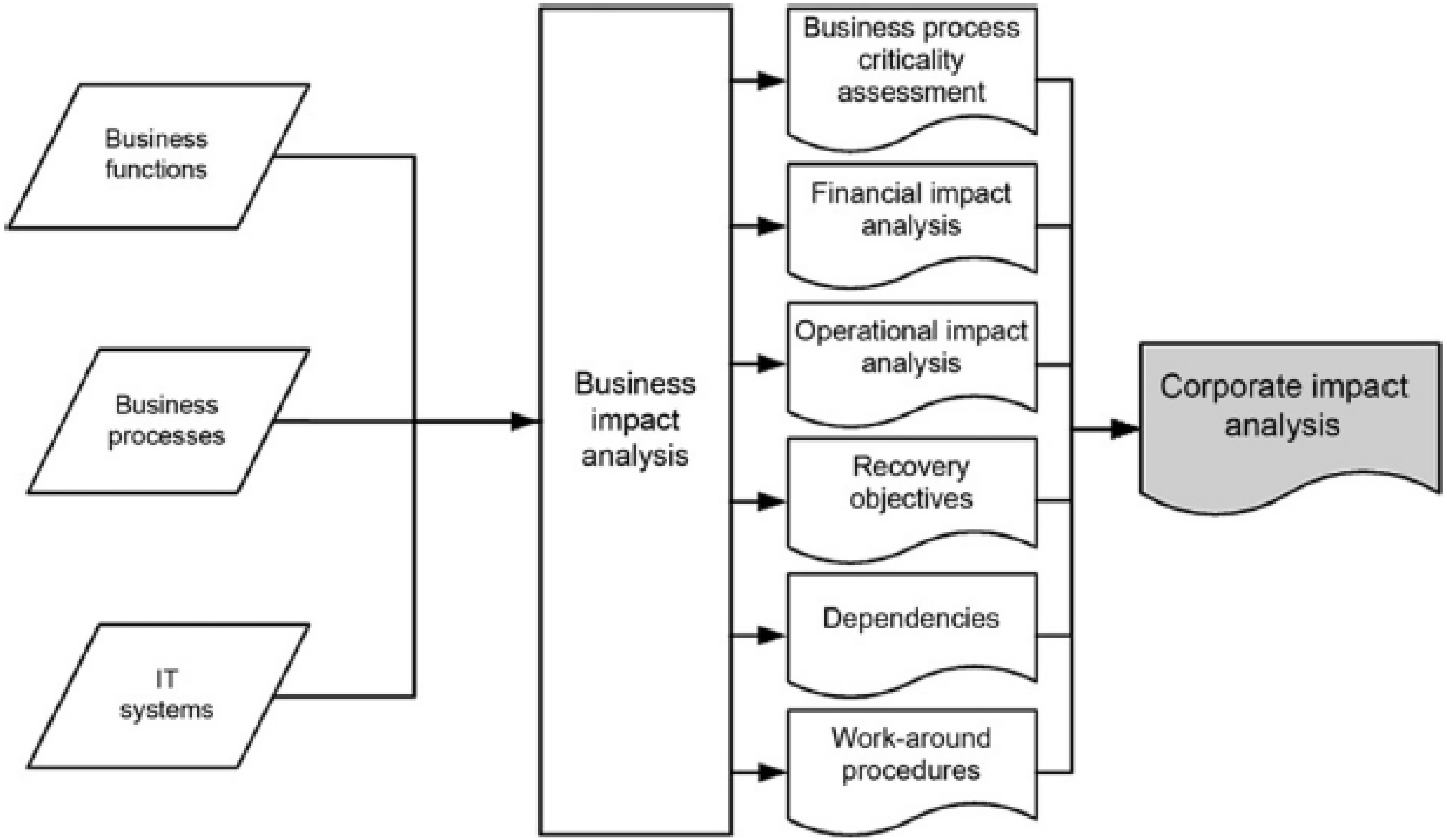


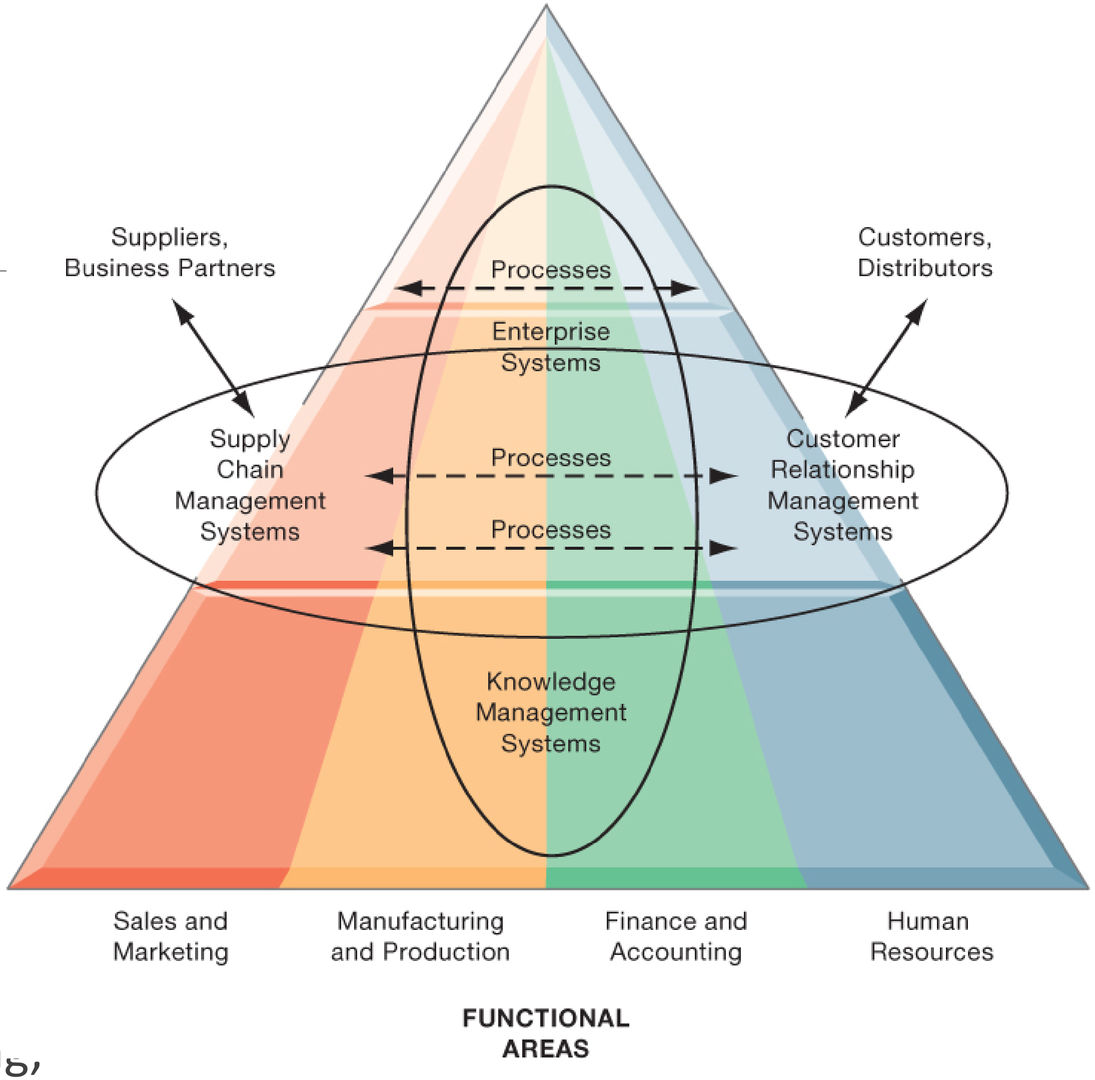
**FIGURE 5.5**

End-to-end business impact analysis.

# Identifying Business Functions

Common business functions

1. Facilities Management
2. Physical Security
3. Finance
4. Human Resources
5. Information Technology
6. Legal/Compliance
7. Manufacturing (Assembly)
8. Marketing and Sales
9. Operations
10. Research and Development
11. Warehouse (Inventory, Order Fulfillment, Shipping, Receiving)


Suppliers, Business Partners
Customers, Distributors
Processes
Enterprise Systems
Supply Chain Management Systems
Processes
Processes
Customer Relationship Management Systems
Knowledge Management Systems
Sales and Marketing
Manufacturing and Production
Finance and Accounting
Human Resources
FUNCTIONAL AREAS

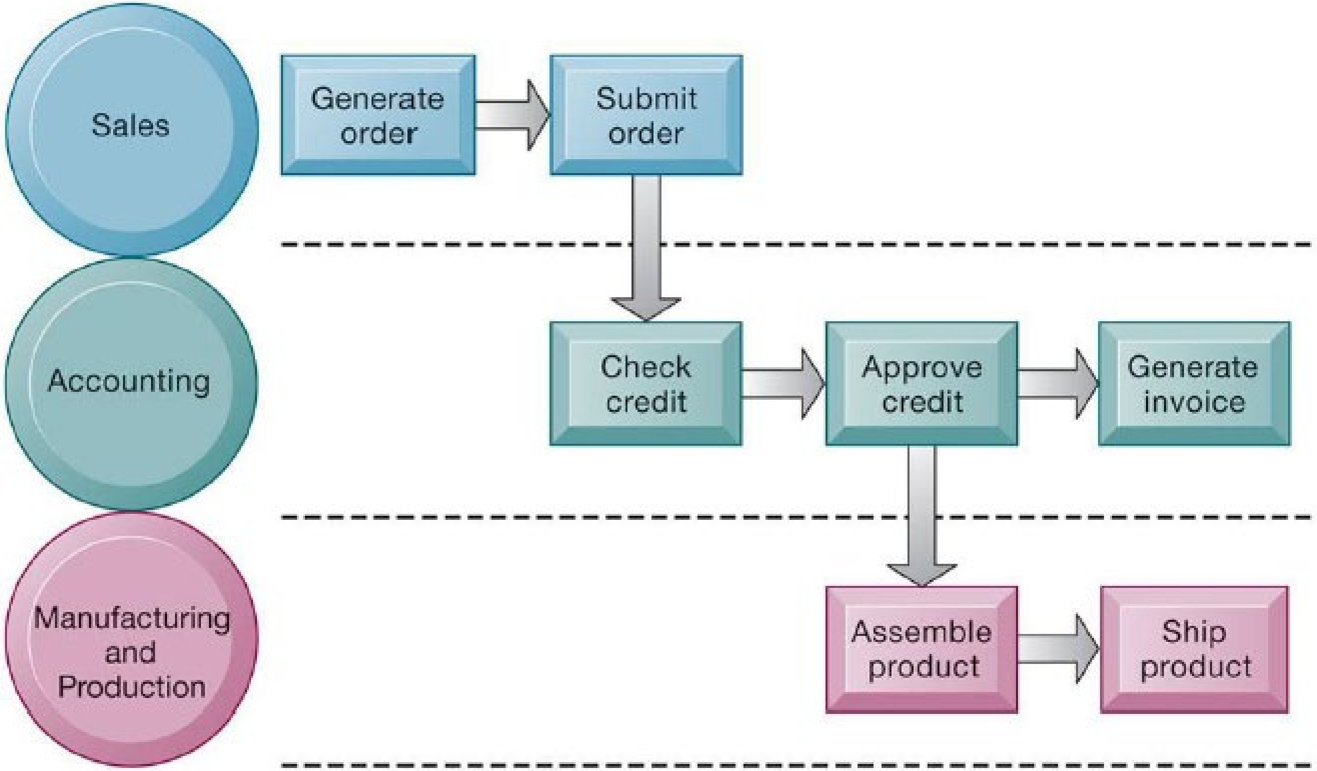
Enterprise Application Architecture (Laudon & Laudon, 2020)

# Identifying Business Functions

There are many inter-depencies in financial functions that cross over into HR, marketing, sales, IT, and operations.

If key IT systems were to go down, which business processes would be impacted?

Which processes and functions would have to get back up and running first in order to keep the business going?



Order Fulfillment Process
(Laudon & Laudon, 2020)

# Identifying Business Functions

Managing security is another critical aspect.

In the aftermath of a major event or disaster, there’s a tendency to “just get it done.”

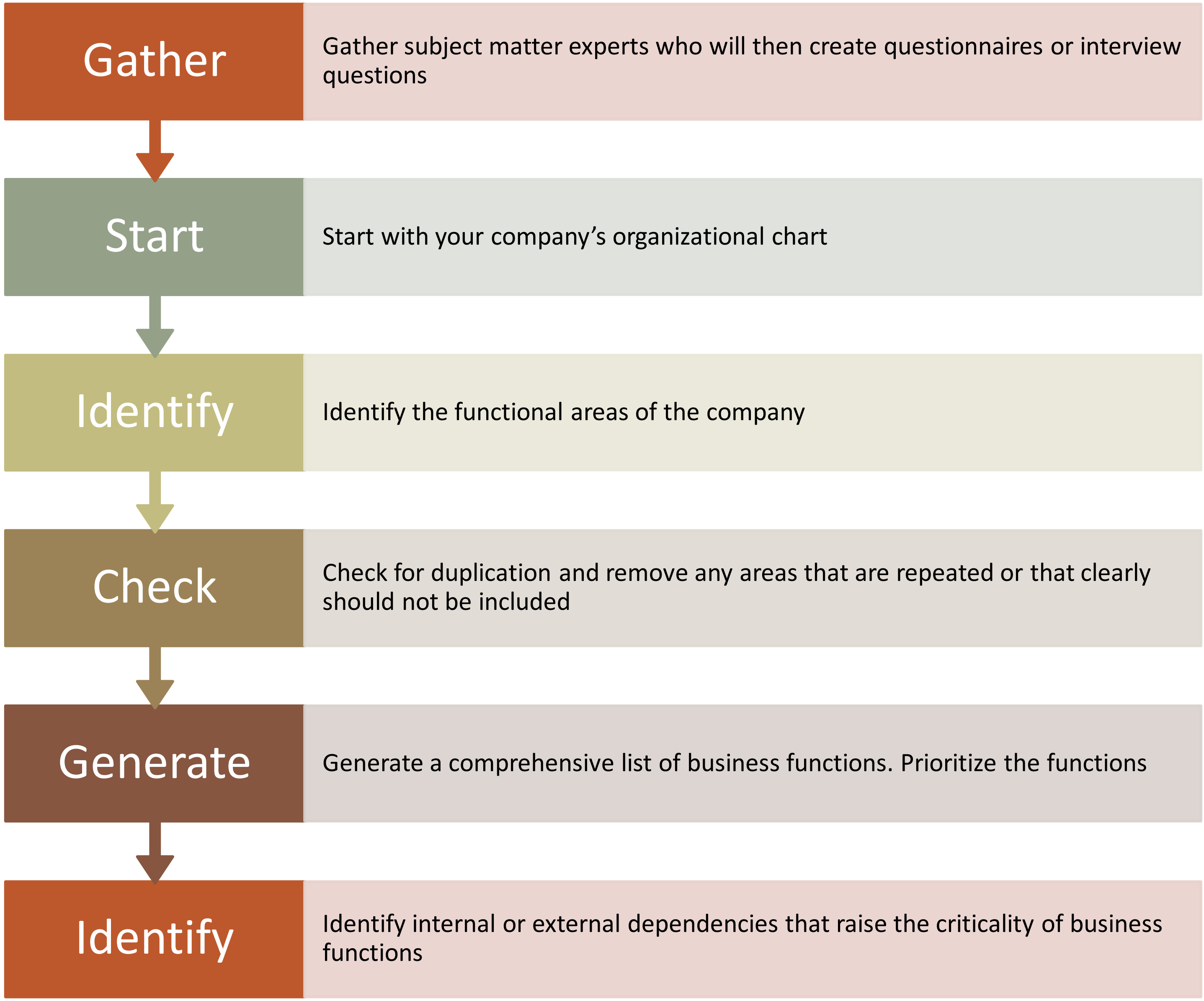
However, ensuring the confidentiality, integrity, and availability of critical business data must still be a top priority.

As with all information security functions, you’ll need to balance security with operational needs.

Still, these are areas to consider as you develop your BC/DR plan and topics to discuss during the BIA process.

# Gathering data for BIA

# Gathering Data for BIA



Gather

Gather subject matter experts who will then create questionnaires or interview questions

Start

Start with your company’s organizational chart

Identify

Identify the functional areas of the company

Check

Check for duplication and remove any areas that are repeated or that clearly should not be included

Generate

Generate a comprehensive list of business functions. Prioritize the functions

Identify

Identify internal or external dependencies that raise the criticality of business functions

# Gathering Data for BIA

Before conducting BIA, you should prepare the following:

- Detailed description of key systems, databases, and information processes, organized by functional area
- Clear description of system interdependencies, interfaces, and upstream/downstream systems
- Identification of IT application owners and their operational counterparts
- Qualitative and quantitative cost descriptions of downtime

# Questions to ask to focus on BIA key aspects

1. How would the department function if desktops, laptops, servers, e-mail, and Internet access were not available?
2. What single points of failure exist? What, if any, risk controls or risk management systems are currently in place?
3. What are the critical outsourced relationships and dependencies? What are the upstream and downstream risks to your business function?
4. If a business disruption occurred, what workarounds would you use for your key business processes?
5. What is the minimum number of staff you would need and what functions would they need to carry out?
6. What are the key skills, knowledge, or expertise needed to recover? What are the key roles that must be present for the business to operate?
7. What critical security or operational controls are needed if systems are down?
8. How would this business function in a backup recovery site? What would be needed in terms of staff, equipment, supplies, communications, processes, and procedures?

# Data Collection Methodologies (1 of 2)

## Questionnaires

- Appropriately design the questionnaire.
- Explain the purpose of the questionnaire to the participants
- Let participants know how they'll learn about the results of the questionnaire
- Review them to ensure they are complete
- Any follow-up interviews should follow a specific format as well so that targeted data can be collected

## Interviews

- Prepare interview questions
- Find the right person or team to conduct the interviews
- Once an interview is conducted, the data need to be reviewed and verified by the interviewee.

# Data Collection Methodologies (2 of 2)

## Workshops or focus groups

- Identify and gain agreement from participants.
- Choose an appropriate time and place for the workshop, ensure the appropriate amenities will be available (white boards, refreshments, etc.)
- Develop a clear agenda for the meeting and distribute this, in advance, to participants. •
- Identify the workshop facilitator and clearly define his or her role in the process. The facilitator’s job is to ensure the workshop objectives are met, so these objectives must be clearly articulated prior to the start of the workshop
- Identify workshop completion criteria so the facilitator and participants are clear about what is expected, what the required outcomes are, and how the workshop will conclude.

## Document reviews

- Review documents to get input about each business functions, review incident handling reports to know which business functions with more incidents, etc.

# Determining the impact

# Determining the Impact (1 of 3)

The impact of any business disruption may include:

1. **Financial.** Loss of revenues, higher costs, potential legal liabilities with financial penalties.
2. **Customers and suppliers.** You may lose customers and suppliers due to your company's problems or you may lose customers or suppliers if they experience a business disruption or disaster.
3. **Employees and staff.** You may lose staff from death, injury, stress, or a decision to leave the firm in the aftermath of a significant business disruption or natural disaster. What are the key roles, positions, knowledge, skills,and expertise needed?
4. **Public relations and credibility.** Companies that experience business disruptions due to IT systems failures (lost or stolen data, modified data, inability to operate due to missing or corrupt data,etc.) have a serious public relations challenge in front of them. These kinds of failures require a well-thought-out PR plan to help support business credibility. What impact would system outages or data losses have on your public image?

# Determining the Impact (2 of 3)

5. **Legal.** Regulations regarding worker health and safety, data privacy and security, and other legal constraints need to be assessed.
6. **Regulatory requirements.** You may be unable to meet minimum regulatory requirements in the event of certain business disruptions.
7. **Environmental.** Some companies may face environmental challenges if they experience failures of certain systems. Understanding the environmental impact of system and business failures is part of the business impact analysis phase.
8. **Operational.** Clearly operations are impacted by any business disruptions. These must be identified and ranked in terms of criticality.
9. **Human Resources.** How will staff be impacted by minor and major business disruptions?
10. **Loss Exposure.** What types of losses will your company face? (property loss, revenue loss, fines, cash flow, accounts receivable, accounts payable.
11. **Social and corporate image**
12. **Financial community credibility.**

# Determining the Impact (3 of 3)

After you’ve compiled a list of your business functions and processes, you should assign a criticality rating to them. You might end up with a table or matrix that looks something like that shown in Table 5.1

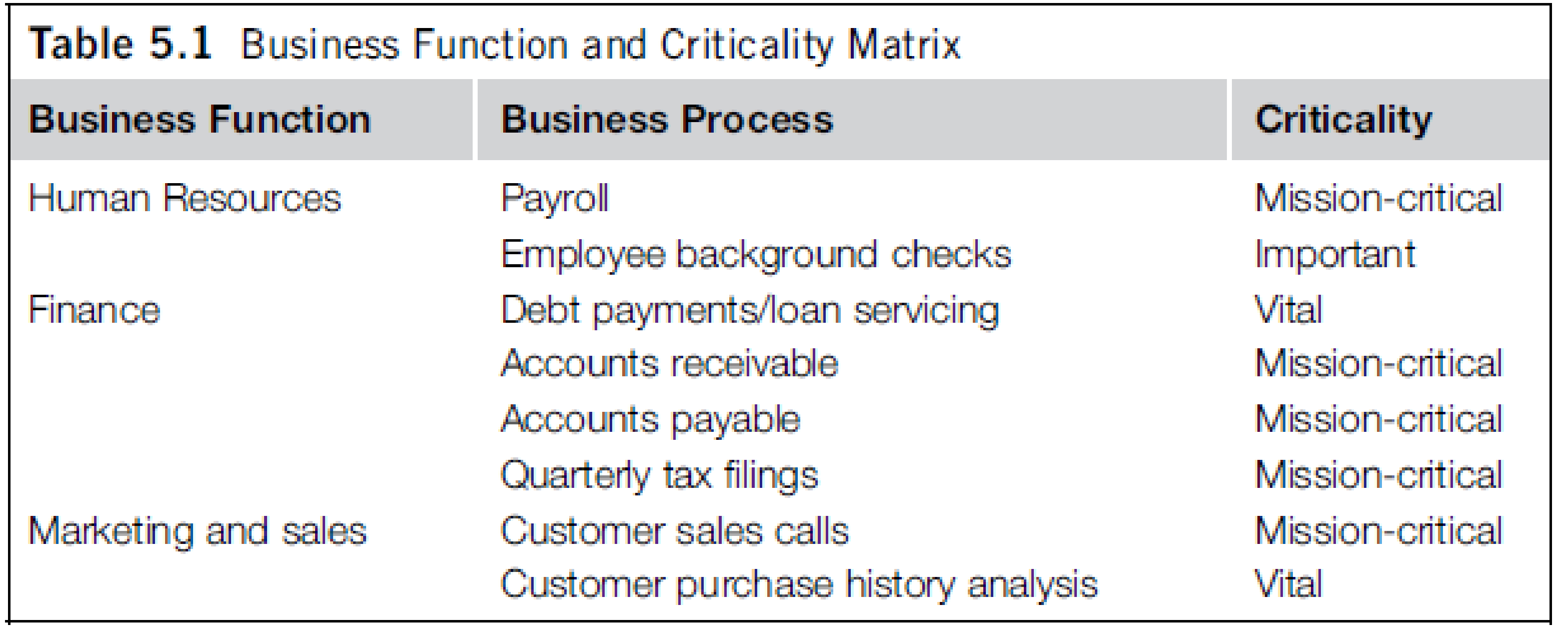


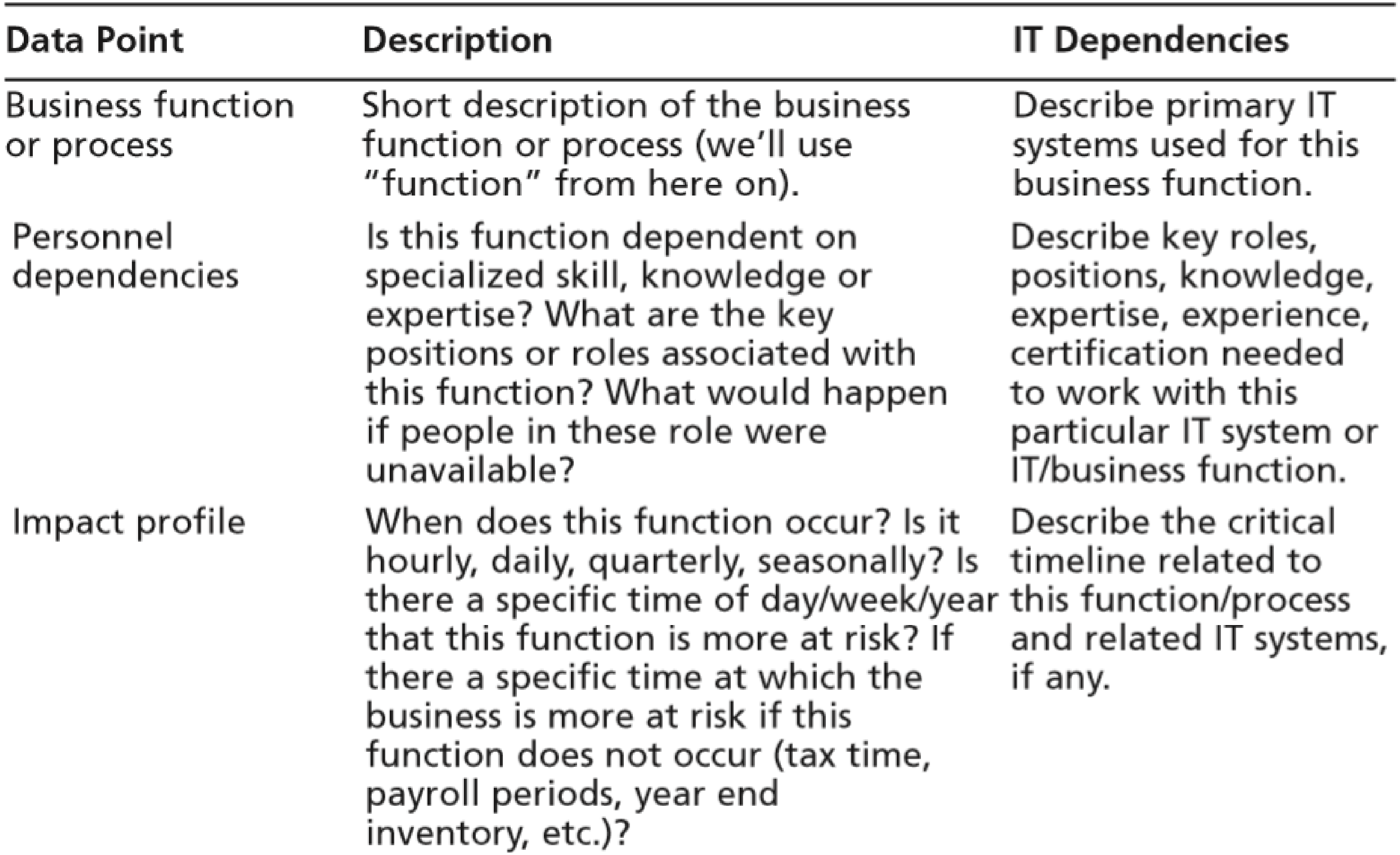
**Table 5.1** Business Function and Criticality Matrix

| Business Function | Business Process | Criticality |
|---|---|---|
| Human Resources | Payroll | Mission-critical |
| | Employee background checks | Important |
| Finance | Debt payments/loan servicing | Vital |
| | Accounts receivable | Mission-critical |
| | Accounts payable | Mission-critical |
| | Quarterly tax filings | Mission-critical |
| Marketing and sales | Customer sales calls | Mission-critical |
| | Customer purchase history analysis | Vital |

# BUSINESS IMPACT ANALYSIS DATA POINTS

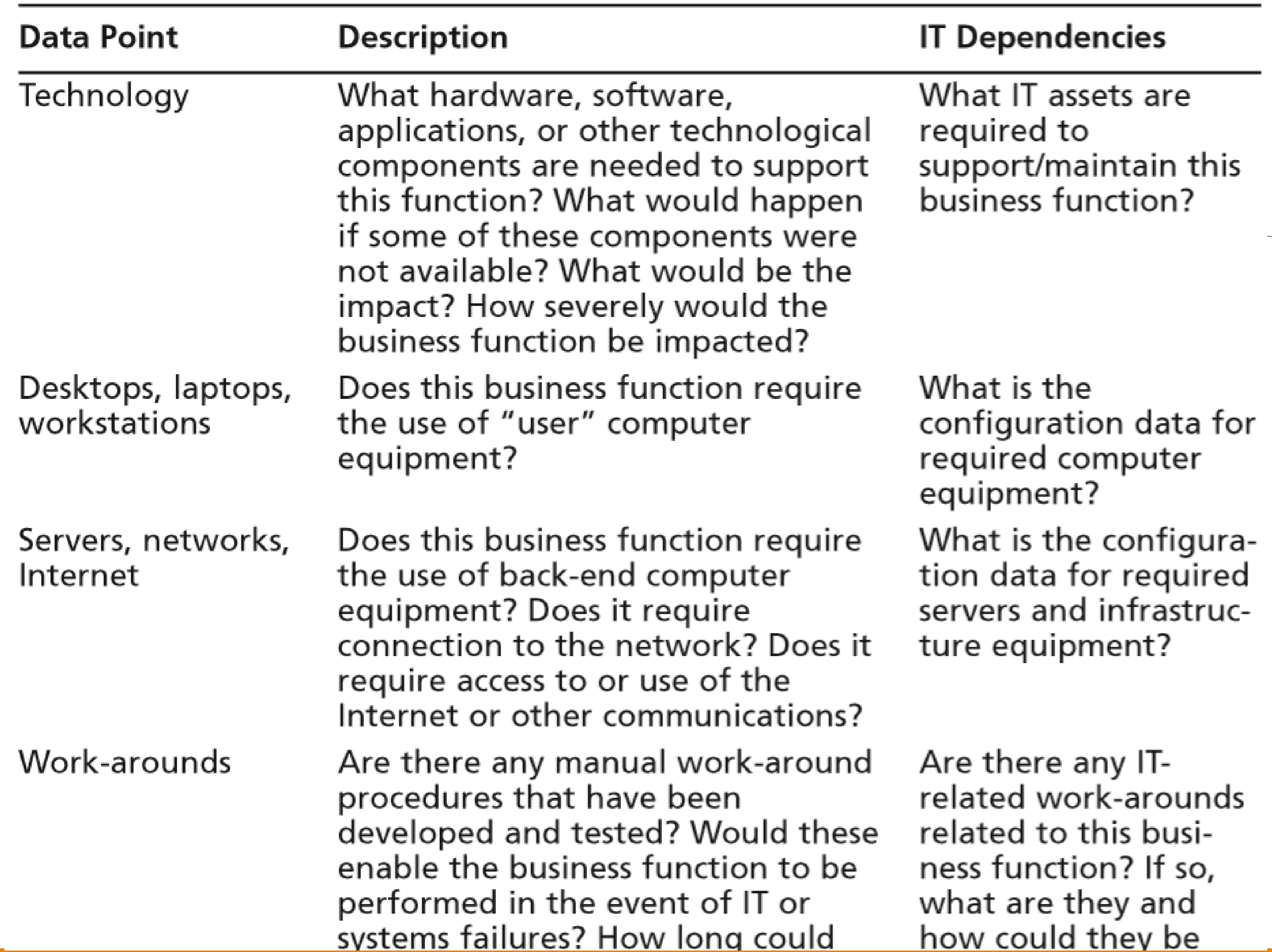
THE NUMBER AND TYPE OF DATA POINTS YOU COLLECT IN YOUR BIA ARE LARGELY A FUNCTION OF THE SIZE AND TYPE OF COMPANY IN WHICH YOU WORK. SMALLER COMPANIES WILL HAVE FEWER DATA POINTS, LARGER COMPANIES WILL HAVE MANY MORE.

# BIA DATA POINTS



| Data Point | Description | IT Dependencies |
|---|---|---|
| Business function or process | Short description of the business function or process (we'll use "function" from here on). | Describe primary IT systems used for this business function. |
| Personnel dependencies | Is this function dependent on specialized skill, knowledge or expertise? What are the key positions or roles associated with this function? What would happen if people in these role were unavailable? | Describe key roles, positions, knowledge, expertise, experience, certification needed to work with this particular IT system or IT/business function. |
| Impact profile | When does this function occur? Is it hourly, daily, quarterly, seasonally? Is there a specific time of day/week/year that this function is more at risk? If there a specific time at which the business is more at risk if this function does not occur (tax time, payroll periods, year end inventory, etc.)? | Describe the critical timeline related to this function/process and related IT systems, if any. |

# BIA DATA POINTS



| Data Point | Description | IT Dependencies |
|---|---|---|
| Technology | What hardware, software, applications, or other technological components are needed to support this function? What would happen if some of these components were not available? What would be the impact? How severely would the business function be impacted? | What IT assets are required to support/maintain this business function? |
| Desktops, laptops, workstations | Does this business function require the use of "user" computer equipment? | What is the configuration data for required computer equipment? |
| Servers, networks, Internet | Does this business function require the use of back-end computer equipment? Does it require connection to the network? Does it require access to or use of the Internet or other communications? | What is the configuration data for required servers and infrastructure equipment? |
| Work-arounds | Are there any manual work-around procedures that have been developed and tested? Would these enable the business function to be performed in the event of IT or systems failures? How long could | Are there any IT-related work-arounds related to this business function? If so, what are they and how could they be |

# Preparing the BIA Report

# Preparing the BIA Report

There is no standardized format for a BIA report

The report should include the business functions, the criticality and impact assessments and MTD assessment for each function

Dependencies, both internal and external, and the correlation to IT systems should be noted

Prepare a draft with initial impact findings and issues to be resolved

BC/DR team members should review the findings. Schedule a review meeting to discuss the findings

Revise the report based on participant’s feedback

Finalize the document

BIA report is used along with the risk assessment as an input to the risk mitigation process

# Elements of BIA Report

Key processes and functions

Process and resource interdependence

IT dependencies

Criticality and impact on operations
Backlog information

Key roles, positions, skills, knowledge, expertise needed

Recovery time requirements

Recovery resources

Service level agreements

- Technology (IT and non-IT)
- Financial, legal, operations, market, staff impacts
- Work-around procedures
- Remote work, workload shifting
- Business data, key records
- Reporting
- Competitive impact
- Investor/market impact
- Customer perception impact

Questions