VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

BCI3002 – Disaster Recovery and Business Continuity Management

(Winter Semester 2022-23)

Enhanced Disaster Recovery and Business Continuity Plan for Small Businesses

Final Review

Submitted To

Dr. Arivoli A

(School of Computer Science and Engineering)

SLOT: C1+TC1

Submitted By:

Rohan Gupta 20BCI0260

Mrinal Sharma 20BCI0247

Harsh Rajpal 20BCI0271

Divyanshi Srivastava 20BCI0166

Satvika Mahapatra 20BCI0289

Shivam Prakash 20BCI0305

Introduction

Natural catastrophes and other exogenous, non-normative shocks to small enterprises are little understood. Additionally, the majority of small business disaster research has, at one point or another, centered on the duality of business recovery. Disaster recovery, however, is an ongoing process for small enterprises that take into account the recovery of each person, their families and households, and their communities over time. It is suggested to use a new dynamic research framework for small business recovery that enables a common structure and terminology.

For small businesses in general, we have presented a business continuity plan and disaster recovery plan that is implemented, with the goals of enhancing RTO and RPO and ensuring operational continuity.

By taking these actions, you can safeguard your small business against potential disasters. If you think your company is particularly vulnerable to disaster, you might think about hiring a disaster recovery expert.

It may seem wasteful to devote your time and resources to a potential threat that may never materialize. Yet, every minute you spend getting ready for a catastrophe translates into an hour saved later on.

Problem Statement

Improving the business continuity and disaster recovery plans (DRPs) for small businesses, especially those with limited resources.

Nothing is more stressful than working tirelessly to make your business profitable just to watch as outside factors like a hurricane, fire, or cyberattack suddenly make it unusable. What's worse is that calamities can seriously harm small enterprises. 90% of small businesses that don't reopen within five days following a tragedy fail within a year, and between 40 and 60% of small firms that experience a crisis never reopen their doors. Small business owners must therefore develop and keep their disaster recovery strategy up to date.

Literature Survey

S.No	Title	Summary and Conclusion	Limitations and Drawbacks
1.	Kato, Mio, and Teerawat Charoenrat. "Business continuity management of small and medium-sized enterprises: Evidence from Thailand." *International journal of disaster risk reduction* 27 (2018): 577-587.	This study helped shed light on Thai SMEs' existing BCM procedures, as well as their obstacles and help requirements. ➢ Despite the fact that Thai SMEs faced many calamities between 2004 and 2014, their readiness for business continuity remained limited or inadequate. ➢ The more catastrophe experiences SMEs had, the better prepared they were. ➢ SMEs that operate on a larger scale or over a longer period of time are more likely to be prepared for disasters, as well as aware of business continuity and training requirements. ➢ The survey revealed that the biggest problems for SMEs in adopting BCM were related to a lack of knowledge and awareness, rather than a lack of funds.	➢ The sampling strategies utilized, particularly questionnaire distribution through personal connections and snowball sampling, might have resulted in sample selection bias. ➢ The survey, which was based on self-evaluation by SMEs, may have resulted in bias or inaccuracy in the measures. ➢ Because BCM is increasingly viewed as a management duty, future studies should include more senior management. ➢ Furthermore, the study was based on small-scale data collected from several businesses, which restricts the generalizability of the findings.
2.	Doern, Rachel. "Entrepreneurship and crisis management: The experiences of small businesses during the London 2011 riots."	This study captures the significant experiences of a specific crisis from the perspective of entrepreneurs, as well as the impact of such on small firms and their reactions. ➢ It documents not just money losses, but also psychological/emotional costs and the setting in which they occur.	➢ One of the study's major drawbacks is that data gathering began two months after the riots. ➢ While the timing allowed for more immediate reactions to the disturbances, it made it impossible to adequately assess the

	International small business journal 34.3 (2016): 276-302.	➢ It examines crisis management activities in small businesses following a riot rather than a natural disaster or industrial crisis, by emphasizing the consequences of a crisis not only for communities but also for businesses and individual owner-managers. ➢ Shows how small organizations may become more resilient and less prone to disasters by drawing on and adapting prior experience, establishing an anticipatory and containment attitude, and investing in and increasing resources.	impact of the riots on the small companies surveyed. ➢ As a result, follow-up interviews with participants should also be done to document the long-term impact of the riots on companies.
3.	After the Fire: An Assessment of Small Business Preparedness and Recovery in Gatlinburg, Tennessee by Sejin Ha, Michelle Childs, Youn-Kyung Kim & Ann Fairhurst for the International Journal of Hospitality & Tourism Administration , 2020.	This study with small business owners and managers in a tourism-dependent community indicated that they continue to struggle with disaster preparedness and recovery planning for natural disasters. ➢ The results revealed a lack of disaster preparedness because small businesses tend to be naïve about the occurrence of natural disasters and they generally focus on day-to-day business operations rather than considering long-term operation management. ➢ Two specific elements important to small businesses' disaster preparedness are (1) support from the parent company of a franchised business and (2) capacity building	➢ This research excluded severely damaged businesses. Since they lack direct business contacts, it was challenging for researchers to make contact with business owners. ➢ These findings are limited to wildfires. Some interviewees indicated the need for emergency preparedness and post-recovery planning by disaster type and, thus, our findings should be considered as a starting point for when planning for or responding to a wildfire.

		through partnerships with others in the community. ➢ Capacity building was a key asset that strengthened their preparedness through strong business-to-business and local community partnerships. ➢ Long Standing community connections became the cornerstone of small business recovery when business managers and owners compiled information about the natural disaster as it occurred, allowing them to respond appropriately and timely.	➢ Lastly, interview data came from interviews conducted with small businesses located in Gatlinburg, TN, which is a small, collaborative, and close-knit community in which the majority of interviewees grew up and knew many community members. Therefore, the results may differ in communities of larger sizes.
4.	Post-disaster business recovery: An entrepreneurial marketing perspective by Morrish, Sussie C.; Jones, Rosalind (2019). for. Journal of Business Research	This paper investigates how Entrepreneurial Marketing (EM) is enacted in post-disaster settings to facilitate speedy business recovery. ➢ They have examined the post-quake experiences of small business entrepreneurs by using inductive research and adopting a 'theories-in-use' approach. ➢ Research propositions have developed that capture the dynamics of the business environment which influence entrepreneurial decisions, actions, and EM behavior. A new definition is offered in the light of this study and an EM PostDisaster Business Recovery (EMPDBR) Framework is provided.	➢ While business recovery has focused on enterprise survival, much of this paper fails to investigate the role and importance of entrepreneurs in business recovery in specific sectors and regions. ➢ Other limitations include the fact that findings are based on a small study in one industry sector and in one city. ➢ The configuration of EM behaviors identified here warrants further examination and testing in different settings and sectors.

		➢ This framework highlights opportunity-seeking, resource-organizing, creating customer value, and accepting risk (ORCAr) as concepts that are markedly different in the post-disaster context.	
5.	R. Solis, N. Shashidhar and C. Varol, "A Novel Risk Mitigation & Cloud-Based Disaster Recovery Framework for Small to Medium Size Businesses," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-5, doi: 10.1109/ISDFS52919.2021.9486373.	❖ They provide a cutting-edge framework that gives small and medium-sized organizations the chance to reduce risk and go on with operations after a calamity. Several recovery options that use a cloud-based storage system are also available. ❖ The findings demonstrate that by enabling users to access backups from any platform or device with web browser capabilities, an ideal recovery time target may be attained. Additionally, a high level of integrity on each client may be attained, reducing the possibility of data loss and revealing financial information to an attacker.	❖ By offering a virtualization approach that produces computers with excellent integrity and availability, they reduce risk. ❖ For each application image, only particular programs and permissions are configured. Our network and data are protected from any potential dangers by restricting connectivity between isolation levels.
6.	Păunescu, C., 2017. How prepared are small and medium-sized companies for business continuity management? *Quality–Access to Success*,	❖ It offers a framework for creating and putting into practice a business continuity management system that complies with international standard ISO 22301 for the quick and painless restoration of vital operations following a disruption.	❖ The research work was limited to Romania only so climate factors can be one of the reasons for the outcomes of this paper. ❖ Only 48 questionnaires were completed which might not be sufficient to evaluate the plan completely.

	18(161), pp.43-48.	❖ 48 questionnaires were asked, demonstrating that the businesses under investigation are aware of what business continuity management is and to some extent contemplate its development and implementation. As a result, only 46% of the organizations studied really assess the many risks or hazards that might result in a disruption of their operation, even if 65% of them recognize them. Additionally, just 25% of the businesses under investigation implement their whole business continuity strategies.	

Phases of Disaster Recovery and Business Continuity Plan

Phase I: Scope and Initiation

Phase 2: Business Impact Analysis

Phase 3: Recovery Strategies and Continuity Development

Phase 4: Implementation and Testing

Phase 5: Maintenance

Phase I: Scope and Initiation

Scope and Initiation is the crucial first step in developing a comprehensive disaster recovery and business continuity plan for small businesses. It involves setting the purpose and scope of the plan, identifying stakeholders and their roles, conducting a risk assessment, defining recovery objectives, developing strategies and plans, establishing a budget and resource plan, and gaining stakeholder buy-in. This phase lays the foundation for the entire plan, ensuring that the small business is well-prepared to mitigate and manage potential disasters and maintain operational continuity in the face of unexpected events. By carefully considering the unique needs and resources of the small business, Phase I sets the stage for effective disaster recovery and business continuity efforts in subsequent phases.

It involves -

- **Establishing the Purpose and Scope:** In this phase, the first step is to clearly define the purpose and scope of the disaster recovery and business continuity plan for small businesses. This involves identifying the key objectives and goals of the plan, as well as understanding the specific needs and requirements of the small business in question. This includes considering the size of the business, its industry, geographical location, and potential risks and vulnerabilities.

- **Identifying Stakeholders and Roles:** The next step is to identify the stakeholders who will be involved in the disaster recovery and business continuity planning process. This may include small business owners, management, employees, external vendors, customers, and other relevant parties. Roles and responsibilities should be clearly defined for each stakeholder, outlining their specific responsibilities during the disaster recovery process and ensuring accountability.

- **Conducting a Risk Assessment:** A thorough risk assessment is a crucial part of the scope and initiation phase. This involves identifying potential risks and vulnerabilities that the small business may face, such as natural disasters, cyber-attacks, power outages, or other disruptions. The risk assessment should consider the likelihood and impact of each potential risk, and prioritize them based on their severity.

- **Defining Recovery Objectives:** Once the risks have been identified and prioritized, the next step is to define the recovery objectives. These objectives should be specific, measurable, achievable, relevant, and time-bound (SMART). Recovery objectives may include minimizing downtime, ensuring data integrity, restoring critical operations, and safeguarding the safety and well-being of employees and customers.

- **Developing Strategies and Plans:** Based on the identified risks, vulnerabilities, and recovery objectives, strategies and plans should be developed to mitigate and manage potential disasters. This may include creating emergency response plans, backup and data recovery plans, communication plans, employee safety plans, and other relevant plans. These strategies and plans should be comprehensive, practical, and flexible, taking into account the unique needs and resources of the small business.

- **Establishing a Budget and Resource Plan:** Another crucial aspect of the scope and initiation phase is to establish a budget and resource plan for implementing the disaster recovery and business continuity plan. This includes identifying the financial resources required for the plan, as well as the necessary personnel, equipment, and technology. Adequate resources should be allocated to ensure the successful implementation and maintenance of the plan.

- **Gaining Stakeholder Buy-In:** Finally, gaining stakeholder buy-in is critical for the success of the disaster recovery and business continuity plan. This involves obtaining support and commitment from all relevant stakeholders, including small business owners, management, employees, and external partners. Communication and education efforts should be undertaken to ensure that all stakeholders understand the importance of the plan and their roles in its implementation.

In conclusion, the scope and initiation phase of the disaster recovery and business continuity plan for small businesses involves establishing the purpose and scope, identifying stakeholders and roles, conducting a risk assessment, defining recovery objectives, developing strategies and plans, establishing a budget and resource plan, and gaining stakeholder buy-in. This phase sets the foundation for the overall plan and ensures that the necessary groundwork is laid for effective disaster recovery and business continuity efforts.

Phase 2: Business Impact Analysis

A. The table below summarizes business analysis for loss of Material.

Potential Causes	Potential Consequences
● Inadequate resources (human and/or technological) ● Inadequate internal control system ● Inadequate backup and archiving processes ● Security breaches ● Fire, Flooding, or structural failure	● Loss of revenue ● Owner dissatisfaction ● Customer Dissatisfaction ● Creation of liabilities ● Drain on resources

Control environment overview

Existing control measures	Recommended additional control measures
● Restricted access to business rooms ● System Data backups ● Uninterrupted power supplies ● Manage and administrative systems	● Physical security controls to ensure that unauthorized access is prevented ● Service level agreements need to be reviewed for all critical areas ● Automated suppression systems need to be implemented ● Configuration and change management ● Generators must be installed for all sites.

B. The table below summarizes the business analysis for the loss of key dependencies:

Potential Causes	Potential Consequences
● Inadequate supplier resources (human and/or technological) ● Inadequate internal control systems ● Breaches of security ● Fire ● Flooding ● Structural failure	● Loss of assets ● Inability to provide services ● Legal penalties ● Drain on resources ● Reputation risk ● Additional on-going costs ● Action by regulators

Content environment overview	
Existing control measure	Recommended additional control measures
● Smoke detection ● Fire suppression systems ● Restricted access to official areas ● Ups battery backup	● Combined business continuity planning and testing with key suppliers ● Generators need to be installed for all hosting facilities to ensure a continuous supply of power ● Operating procedures and check-list to reduce reliance on individuals and suppliers ● Automated fire suppression systems need to be implemented ● Physical security controls need to be improved ● Service-level agreements need to be reviewed and implemented

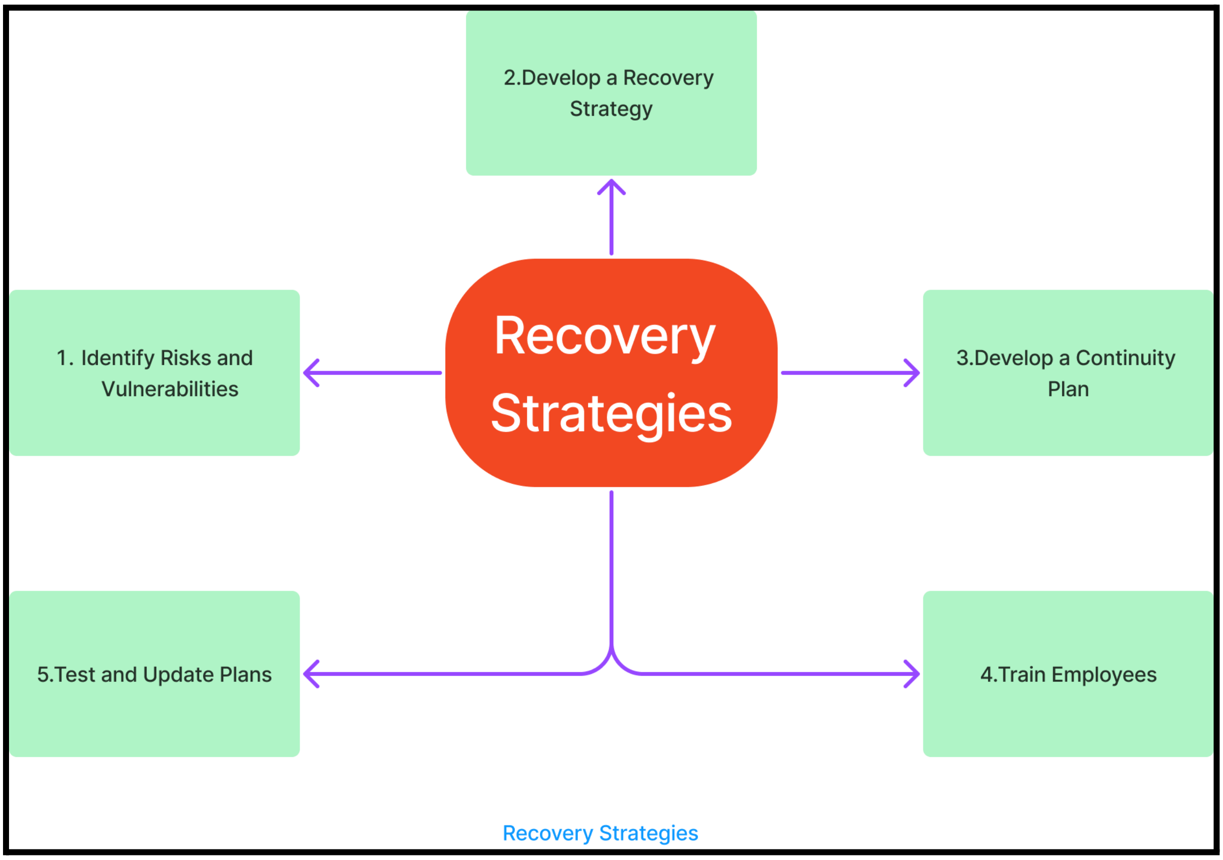
C. The table below summarises the business analysis for the loss of key staff:

Potential Causes	Potential Consequences
● Breaches of physical security ● Biological threat	● Loss of knowledge ● Reduced productivity

● Injury or illness ● Resignation	● Drain on resources ● Additional ongoing costs

Constant Environment Overview	
Existing control measure	Recommended additional control measures
● Detailed job descriptions and performance agreements ● Good knowledge transfer between staff is happening ● Security at the main entrance and building entrances	● Note: Municipality should apply to both ICT staff and operations staff: ● Succession planning for key staff ● Improve turnaround time to acquire resources ● Stander's operating procedures to reduce reliance on individuals and suppliers ● The hiring of additional staff ● Outsourcing of some functions ● Standard agreements with recruitment agencies ● Security needs to verify the identity of visitors.

Phase 3: Recovery Strategies and Continuity Development


2.Develop a Recovery Strategy
1. Identify Risks and Vulnerabilities
Recovery Strategies
3.Develop a Continuity Plan
5.Test and Update Plans
4.Train Employees
Recovery Strategies

Recovery Strategies:

Any occurrence that has the potential to significantly influence critical operations and/or PC handling capabilities for a prolonged length of time is referred to as a "disaster" and would have an impact on the CA company.

The goal of explaining a crisis or anomaly is to give a reported image of what triggers a crisis or a malfunction. Having a few alternatives as possible when a circumstance arises is the aim. Two systems have been put up, one for the immediate future and the other for the long term. You can read more about both of these strategies in the archive.

They are susceptible to several dangers, such as pandemics, natural catastrophes, cyberattacks, and economic downturns. Small companies must have a recovery strategy and continuous development plan in place in the case of a disruption to limit the effects on their operations and guarantee that they can continue to service their clients.

Various recovery strategies are available:

1. **Identify risks and vulnerabilities:**

   The process of creating a recovery strategy and continuity plan begins with the identification of potential risks and weaknesses that could have an impact on the company's operations. Natural catastrophes like floods or hurricanes, cyberattacks, supply chain disruptions, or economic downturns might all be among these threats. After these risks have been recognized, small firms should give them the priority and create plans to reduce them.

2. **Develop a Recovery Strategy:**

   A recovery strategy is a blueprint for how a company restarts operations following an interruption. This plan should outline a schedule for operations to resume, an evaluation of the disruption's possible effects, and a list of the resources required to carry it out. Small firms should also take into account the accessibility of backup systems, other work sites, and contingency plans for crucial suppliers and vendors.

3. **Develop a Continuity Plan:**

   A thorough strategy that describes how a firm will carry on during an interruption is known as a continuity plan. An evaluation of the resources required to sustain these operations, a list of the important functions that must continue throughout the interruption, and a communication strategy for staff, clients, and vendors should all be part of this plan. To make sure that crucial operations can continue even if employees are unable to reach the actual office, small firms should also think about putting remote work regulations and backup solutions in place.

4. **Train Employees:**

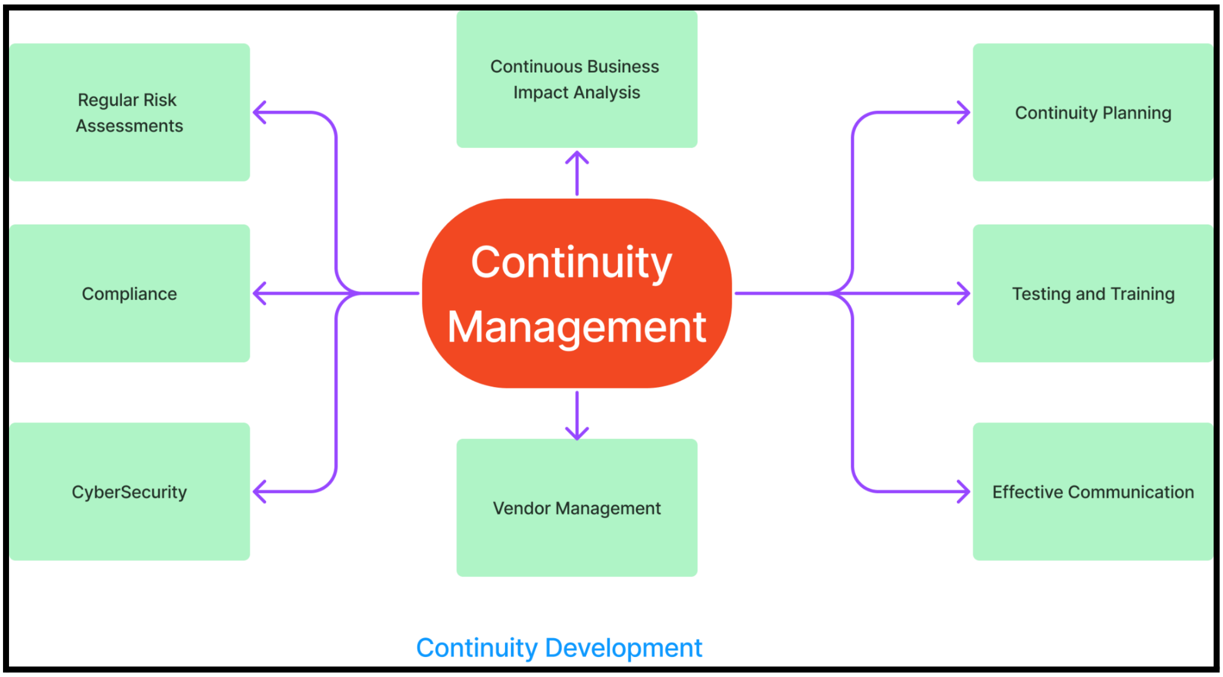
   Workers play a crucial role in a small business' efforts to recover and continue operations. Employees in small organizations should be trained on the recovery and continuity strategy, including their obligations in the event of a disruption. The utilization of backup systems, remote work tools, and how to interact with clients, suppliers, and other stakeholders during disruption should all be covered in this training.

5. **Test and Update Plans:**

   To make sure their recovery and continuity plans are current and effective, small firms should test and revise them frequently. Frequent testing can assist find possible flaws in the strategy and guarantee that staff members are aware of its protocols. Small firms should examine their plans regularly and revise them as necessary to account for changes in the company's operations or potential new hazards.

Continuity development:

The process of enhancing a company's continuity management program over time to keep it current and efficient is known as continuity development. This is crucial for small firms, which may encounter unique difficulties and dangers as they develop and flourish.



Continuity Development

1. **Regular Risk Assessments:**

   The risk assessment should be periodically reviewed and updated to reflect any changes in the business environment as the initial stage in continuity development. Changes to the business's operations, supply chain, or regulatory environment may fall under this category. Potential disruptions like pandemics, cyberattacks, and natural catastrophes should all be taken into account in the risk assessment along with their possible effects on the company.

2. **Continuous Business Impact Analysis:**

   A business impact analysis (BIA) should also be updated often to account for adjustments made to the operations of the company. The vital business processes and functions that are essential to the firm's operations, as well as the resources needed to support them, should be identified by the BIA. This will enable the company to prioritize its efforts for business continuity by better understanding the possible effects of an interruption on its operations.

3. **Continuity planning:**

The company' activities should always be taken into account while updating the continuity plans. This covers recovery methods, business continuity measures, and emergency response protocols. To keep them current and effective, continuity plans for small firms should be reviewed frequently.

4. **Testing and Training:**

   To make sure the continuity plan is functional and that staff members are aware with their duties and responsibilities during a disruption, testing and training should be done on a regular basis. Tabletop activities, simulation exercises, or full-scale rehearsals can all be used for testing. To make sure they continue to be effective, testing and training programmes for small firms should be reviewed and updated on a regular basis.

5. **Effective Communication:**

   During an interruption, effective communication is crucial. To keep it relevant and successful, small businesses should evaluate and update their communication strategy on a regular basis. Contact details, communication channels, communication templates, and communication procedures are all included.

6. **Vendor Management:**

   To make sure that their partners and suppliers can continue to deliver essential products and services in the event of an interruption, small companies should routinely assess and update their vendor management programme. This can entail going over contracts, evaluating supplier risks, and making backup plans.

7. **CyberSecurity:**

   An increasingly crucial component of continuity management is cybersecurity. To guarantee that they continue to be safe from cyber attacks, small companies should assess and update their cybersecurity programme on a regular basis. Regular vulnerability assessments, staff education, and incident response planning may all fall under this category.

8. **Compliance:**

   Several regulatory regulations that may apply to small enterprises may have an influence on their continuity management programme. In order to make sure that the software complies with these standards, it is crucial to evaluate and update it often. Compliance with industry-specific standards, like ISO 22301, or legal obligations, like the General Data Protection Regulation, may be part of this (GDPR).

Phase 4: Implementation and Testing

Implementation

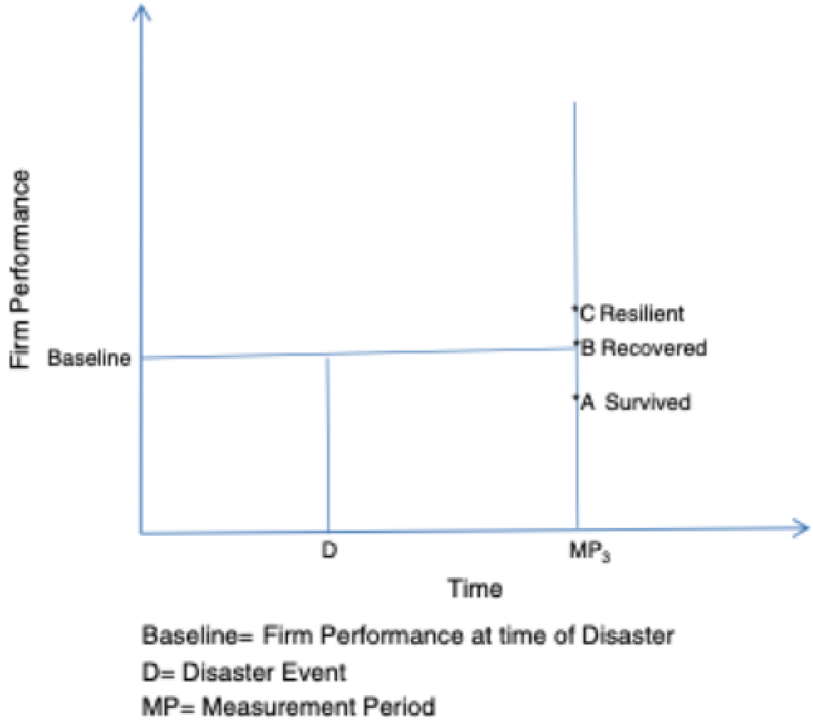
The Small Business Disaster Recovery Framework is founded on the idea that businesses are on a continuum of recovery. A company can be categorised into a certain stage within the process at any time following the disaster event: operational, not operating, demised, survived, resilient or recovered. During the disaster recovery process, a variety of factors, including business characteristics, family and community resources, governmental policy, location, community vulnerability, and social capital influence how businesses move from one stage of recovery to the next over varying lengths of time.

The Small Business Disaster Recovery Framework will assist in addressing crucial and underexplored issues about how catastrophes affect small companies. By placing the criteria on a continuum and focusing attention on the process of recovery or demise that takes place over time, the suggested framework incorporates and improves criteria for company recovery while extending on their conceptions of long-term recovery. It offers a structured framework and a shared terminology to enable scholars who are interested in small company recovery. Researchers will be able to respond to queries like, "Are firms more vulnerable at different phases or times of the recovery process?", “Do some times or stages of government intervention work better than others”, “Do community factors affect small business recovery during the short-term and long-term; and what factors influence the small business recovery process in both positive and negative ways? “

Employers and small businesses with non-disaster SBA loans, from new or current borrowers, are given temporary reprieve from payments under the SBDRF. The following are the SBA's guidelines for borrowers:

The SBA will automatically cover principal, interest, and fee payments for six months for current borrowers with 7(a), 504, or Microloans.

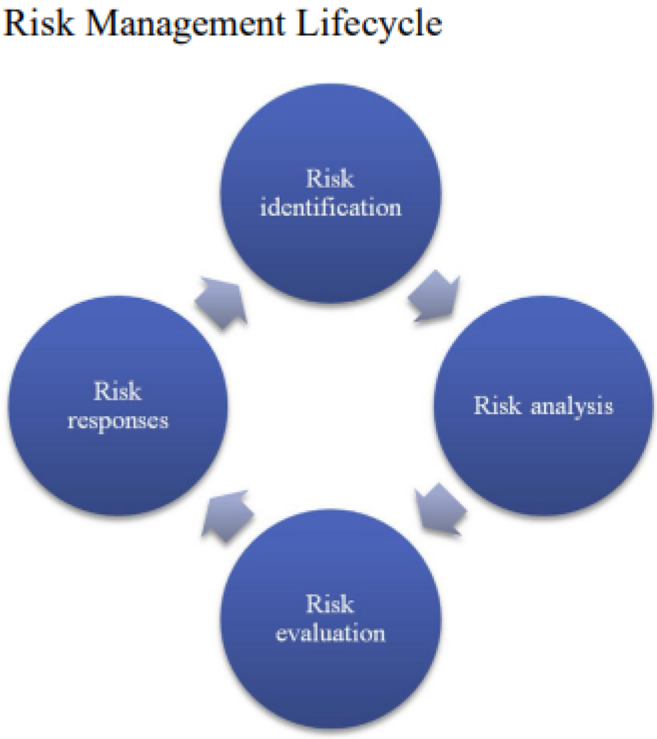
If a new borrower files for and is approved for a 7(a), 504, or Microloan before September 27, 2020, the SBA will pay all loan repayments, including principle, interest, and fees.



As a result, measurement period 1 makes a preliminary determination of whether a business is operating or not. Companies that are not in operation may fall into a number of categories, such as permanently closed or defunct, preparing to reopen, or unknown (i.e., researcher has not located the business or owner at that point in time). The framework simply suggests functioning and non-operational states because it's possible that the information required to establish a meaningful categorization won't be accessible.

Compared to measurement period 1, when a smaller selection of states is required, measurement period 2 requires a greater range of states from which to classify firms. Owner interaction at later measurement intervals allows for more precise measurements. This results in the addition of the states of surviving, recovery, and resilience. Yet, it is still challenging to determine the status of open firms and if they can be described as survived, recovered, or resilient. This is true even though the evidence on whether a business is not operating or demised may be clearer at measurement period 2.

Testing



Identify Risks:

Here are the various types of risks that we have identified in relation to small business.

- Cyber Attacks (Malware, Virus, Phishing, SQL Injection, Denial of Service)
- Natural Disasters (Floods, Earthquake, Tsunamis, Hurricane)
- Man-made threats (Robbery, inside information leak.

Analyse Risks:

Financial

Most disasters will cause some amount of financial loss. But if your leadership team and employees have to scramble to respond, the business is more likely to lose a lot more money.

And the cost of a business-impacting disaster is only increasing. For example, IBM found that in 2016 there had been a seven percent increase in the total cost of a data breach, with a single breach costing U.S. businesses an average of $7.01 million. Other potential crises can be just as costly. It’s no wonder that many companies never recover after being hit by a significant emergency.

Risk probability: High, Risk Recovery: Medium

Operational

A variety of disasters can impact your company’s ability to operate effectively. Imagine which departments and capabilities would be hampered by a flood in your facility. How would your workers manage to do their jobs? How long would it take for customers to be impacted by the operational slowdown? Crises like this can have a ripple effect, gradually impacting all areas of a business in ways that you may have never imagined.

Risk probability: Medium, Risk Recovery: High

Reputational

Of course, a company can also be hurt in indirect ways, such as when the poor handling of a disaster leads to a damaged reputation. In recent years, we’ve seen real-life examples of this in a wide range of crises, such as the Volkswagen emissions scandal and news of Wells Fargo’s fraudulent customer accounts. Reputational damage can impact your bottom line while also hampering future investment, turning away quality employees, and causing other harm— sometimes for years to come.

Risk probability: High, Risk Recovery: Medium

Ever-evolving hacking techniques

If a criminal is going to attempt to infiltrate your company, in many cases, it's more likely that he or she would hack into your IT networks rather than walk through the front door. For most modern businesses, protecting your company starts with safeguarding IT systems.

Risk probability: Medium, Risk Recovery: High

Plan Risk Response:

Set up an emergency response plan and train employees how to carry it out. Make sure employees know whom to notify about the disaster and what measures to take to preserve life and limit property losses. Write out each step of the plan and assign responsibilities to employees in clear and simple language. Practice the procedures set out in the emergency response plan with regular, scheduled drills.

- Compile a list of important phone numbers and addresses:
  Make sure you can get in touch with key people after the disaster. The list should include local and state emergency management agencies, major clients, contractors, suppliers, realtors, financial institutions, insurance agents, and insurance company claim representatives.
- Decide on a communications strategy to prevent loss of customers:
  Post notices outside your premises; contact clients by phone, email, or regular mail; place a notice in local newspapers. Consider the things you may need initially during the emergency. Do you need a back-up source of power? Do you have a back-up communications system?
- Human resources:
  Protect employees and customers from injury on the premises.

Consider the possible impact a disaster will have on your employees' ability to return to work and how customers can return to your shop or receive goods or services.

- Physical resources:
  Inspect your business' plant(s) and assess the impact a disaster would have on facilities. Make sure your plans conform to local building code requirements.
- Business community:
  Even if your business escapes a disaster, there is still a risk that it could suffer significant losses due to the inability of suppliers to deliver goods or services or a reduction in customers. Businesses should communicate with their suppliers and markets (especially if they are selling to a business as a supplier) about their disaster preparedness and recovery plans so that everyone is prepared.
- Protect your building:
  If you own the structure that houses your business, integrate disaster protection for the building as well as the contents into your plan. Consider the financial impact if your business shuts down as a result of a disaster. What would be the impact for a day, a week or an entire revenue period?
- Keep duplicate records:
  Back-up computerised data files regularly and store them off premises. Keep copies of important records and documents in a safe deposit box and make sure they're up-to-date.
  Identify critical business activities and the resources needed to support them. If you cannot afford to shut down your operations, even temporarily, determine what you require to run the business at another location.
- Find alternative facilities, equipment, and supplies, and locate qualified contractors. Consider a reciprocity agreement with another business. Try to get an advance commitment from at least one contractor to respond to your needs. Protect computer systems and data. Data storage firms offer offsite backups of computer data that can be updated regularly via high-speed modem or through the Internet.

Monitor and Control Risk Management Plan:
Develop a risk management strategy that includes identifying potential hazards and putting in place control mechanisms to mitigate such risks. Rank the dangers in order of their importance, as shown above: Prepare a plan to manage and control cyber-attacks, natural disasters, and man-made calamities.

Risk Registers: Maintain a register of each and every probable risk along with additional details. Keep updating the register along with changes that keep happening in the environment. This helps track your risks each and every week.

Phase 5: Maintenance

The maintenance phase of a DRP is just as important as the planning and implementation phases, as it ensures that the plan remains up-to-date and effective.

Here are some key steps to maintain a DRP for small businesses:

1. **Regularly review and update the plan:** A DRP should be reviewed and updated on a regular basis, at least once a year, or whenever there is a significant change in the business environment. During the review, the plan should be checked for accuracy, completeness, and effectiveness. Any changes or updates should be made to reflect new processes, procedures, or technologies that have been implemented since the last review.
2. **Test the plan:** Regular testing of the DRP is essential to ensure that it is effective and that all stakeholders understand their roles and responsibilities in the event of a disaster. Tests can be conducted in the form of tabletop exercises, simulations, or full-scale drills. The purpose of testing is to identify any gaps or weaknesses in the plan and to address them before an actual disaster occurs.
3. **Provide training and awareness:** Regular training and awareness sessions should be conducted for all employees to ensure that they understand the DRP and their roles in the recovery process. This includes training on emergency procedures, data backup and

recovery, and communication protocols. Training should be provided to new employees and refresher training should be provided to all employees on a regular basis.

4. **Backup data and systems regularly:** It is important to regularly back up all critical data and systems to ensure that they can be restored in the event of a disaster. Backups should be stored offsite, preferably in a secure location. The backup process should be tested to ensure that it is working effectively and that all necessary data is being backed up.
5. **Review insurance coverage:** Business owners should review their insurance coverage regularly to ensure that it covers all potential risks and that it is up-to-date. This includes property insurance, liability insurance, and business interruption insurance. Business owners should also review their policy limits to ensure that they are adequate to cover the costs of recovery.
6. **Update contact lists:** Contact lists for key stakeholders, such as employees, customers, suppliers, and emergency services, should be updated regularly to ensure that they are accurate and up-to-date. Contact lists should include phone numbers, email addresses, and physical addresses. This will help ensure that communication can be quickly and effectively established in the event of a disaster.

By following these steps, small businesses can ensure that their DRP remains effective and up-to-date and that they are well-prepared to recover from any disaster that may occur. A well-maintained DRP can help mitigate the impact of a disaster on a small business and help ensure its long-term survival.

Conclusion

Small Businesses make some harder memories recuperating from cataclysmic events contrasted with extremely huge organizations. They are additionally fundamental for the economy and to the general population of the district affected by a catastrophic event, and subsequently, it is significant that we gain a more prominent comprehension of the recovery of small businesses inside the setting of recuperation of people, families, the fabricated climate, and the social local area.

We can clearly see that the implementation of our Disaster Recovery and Business Continuity Plan will help researchers address important and understudied questions regarding the impact of disasters on small businesses such as:-

1. Are organizations more powerless during specific stages or times of the recuperation cycle?
2. Does accomplishing government mediation work best during certain periods or stages rather than others?
3. Do local area factors influence small business recovery during the present moment and long haul; and what elements impact the private venture recuperation process in both positive and negative ways?

References

1. Kato, Mio, and Teerawat Charoenrat. "Business continuity management of small and medium-sized enterprises: Evidence from Thailand." *International Journal of disaster risk reduction* 27 (2018): 577-587.
2. Doern, Rachel. "Entrepreneurship and crisis management: The experiences of small businesses during the London 2011 riots." *International small business journal* 34.3 (2016): 276-302
3. Morrish, Sussie C.; Jones, Rosalind (2019). Post-disaster business recovery: An entrepreneurial marketing perspective. *Journal of Business Research*
4. Ha, Sejin; Childs, Michelle; Kim, Youn-Kyung; Fairhurst, Ann (2020). After the Fire: An Assessment of Small Business

Preparedness and Recovery in Gatlinburg, Tennessee. *International Journal of Hospitality & Tourism Administration.*

5. R. Solis, N. Shashidhar and C. Varol, "A Novel Risk Mitigation & Cloud-Based Disaster Recovery Framework for Small to Medium Size Businesses," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-5, doi: 10.1109/ISDFS52919.2021.9486373.
6. Păunescu, C., 2017. How prepared are small and medium-sized companies for business continuity management? *Quality–Access to Success*, *18*(161), pp.43-48.