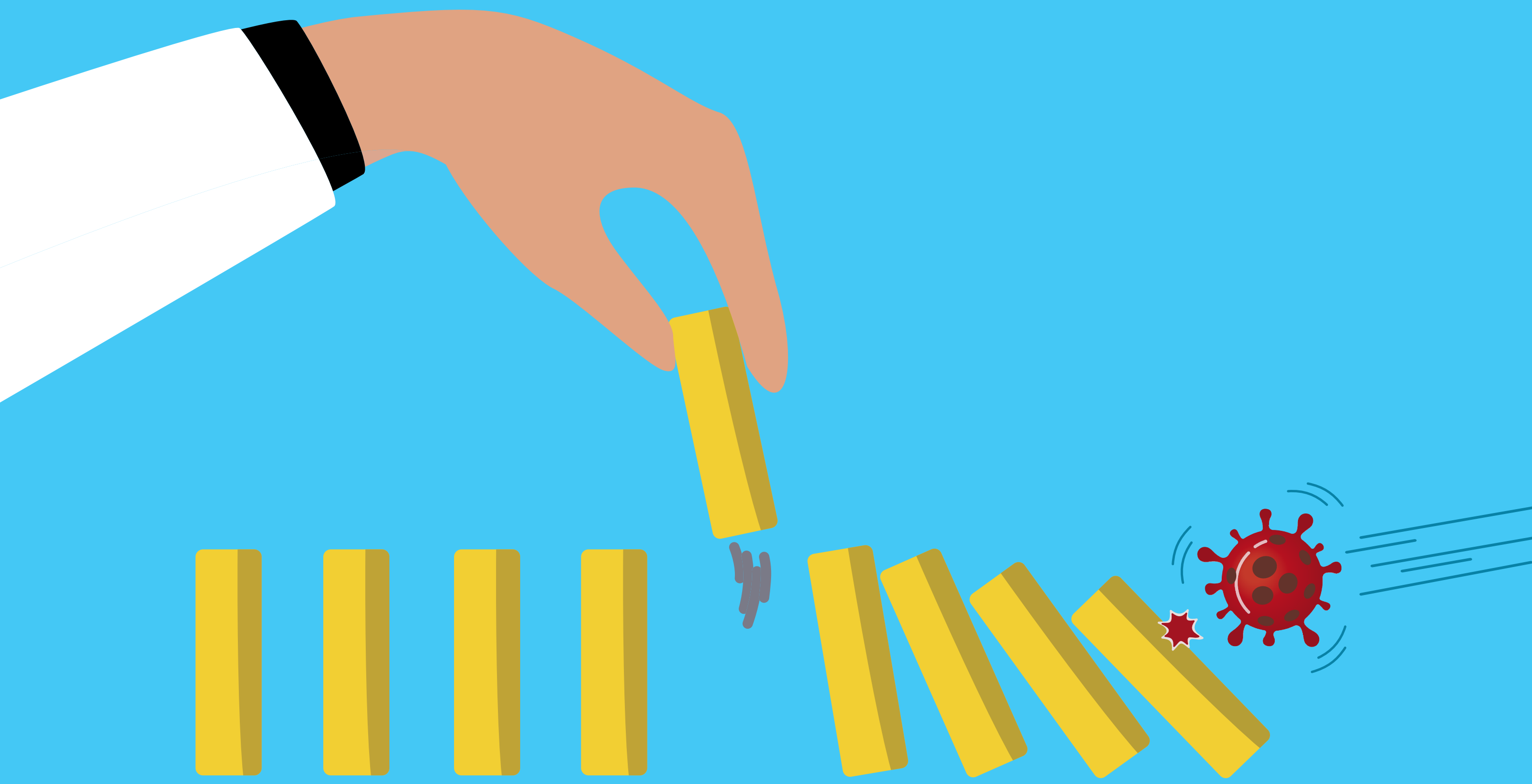
BUSINESS CONTINUITY & DISASTER RECOVERY HANDBOOK

How Zohocorp responds to disasters and does business as usual

Featuring

- BCDR framework for enterprises.
- A Covid-19 case study: Dealing with the new business normal - working from home



“You can’t predict the next catastrophe, but you can be prepared for it!”

ZOHO

Glossary of terms

ARMC	Audit and risk management committee
BC	Business continuity
BCC	Business continuity coordinators
BCDR	Business continuity and disaster recovery
BCM	Business continuity management
BCDRC	Business continuity and disaster recovery committee
BIA	Business impact analysis
COVID-19	Commonly known as coronavirus; a global pandemic which is a severe acute respiratory syndrome
DR	Disaster recovery
Disaster recovery team	Disaster recovery team
Emergency management team	Emergency management team
Building management system	Building management system

Open the book & find

Chapter 01

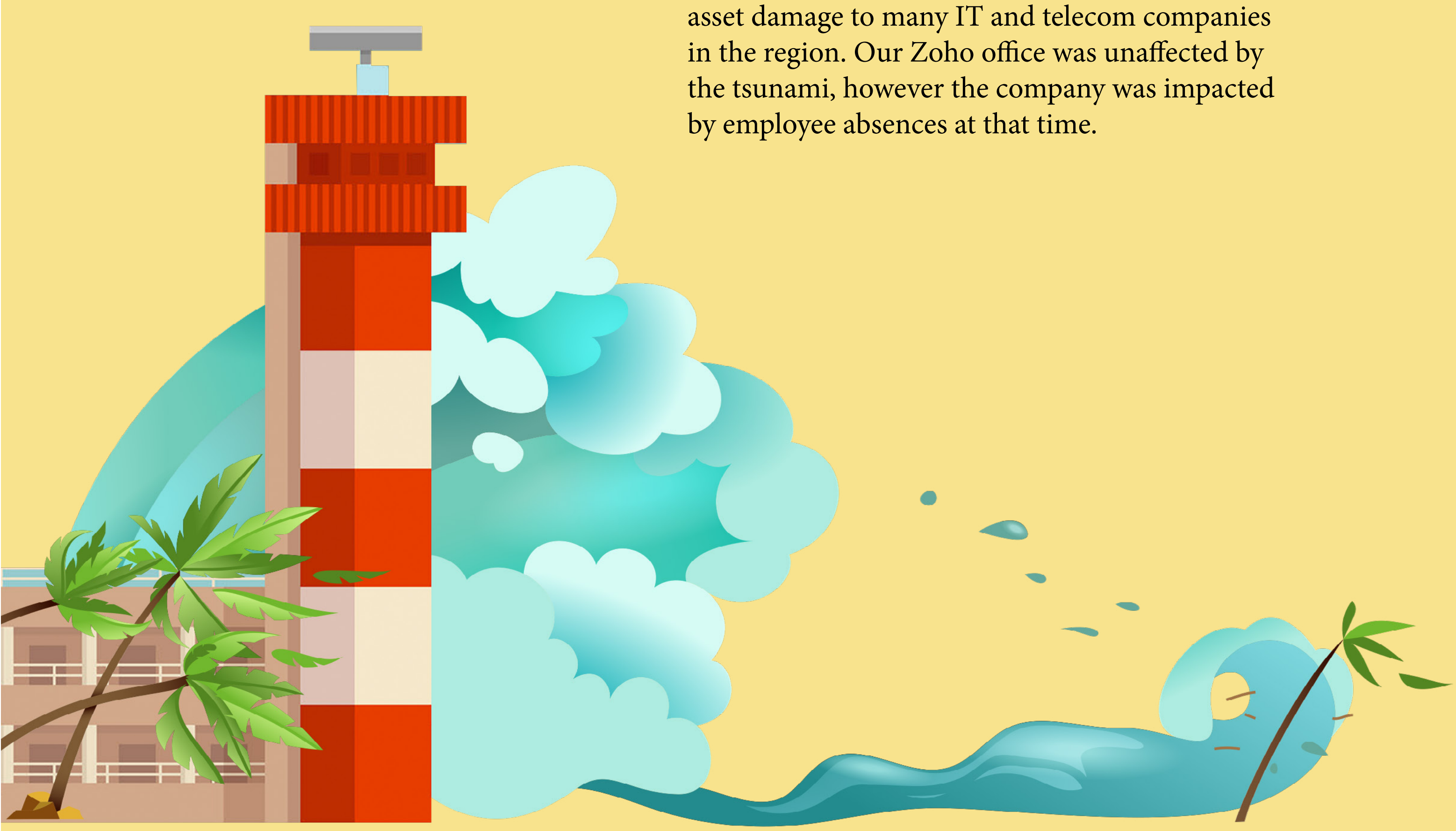
Introduction

Backstory:
The realization

Tsunami in 2004

Before and during the 90s, the city of Chennai was a peace haven and not vulnerable to natural disasters. However, over the last decade, we've witnessed natural disasters in all forms—hurricane, earthquake, tsunami, and the recent global viral pandemic COVID-19.

In 2004, a magnitude 9.1 earthquake struck beneath the Indian Ocean near Indonesia, generating a massive tsunami that claimed around 8,000 lives in coastal Chennai. The giant waves flooded the seaside areas causing property and asset damage to many IT and telecom companies in the region. Our Zoho office was unaffected by the tsunami, however the company was impacted by employee absences at that time.

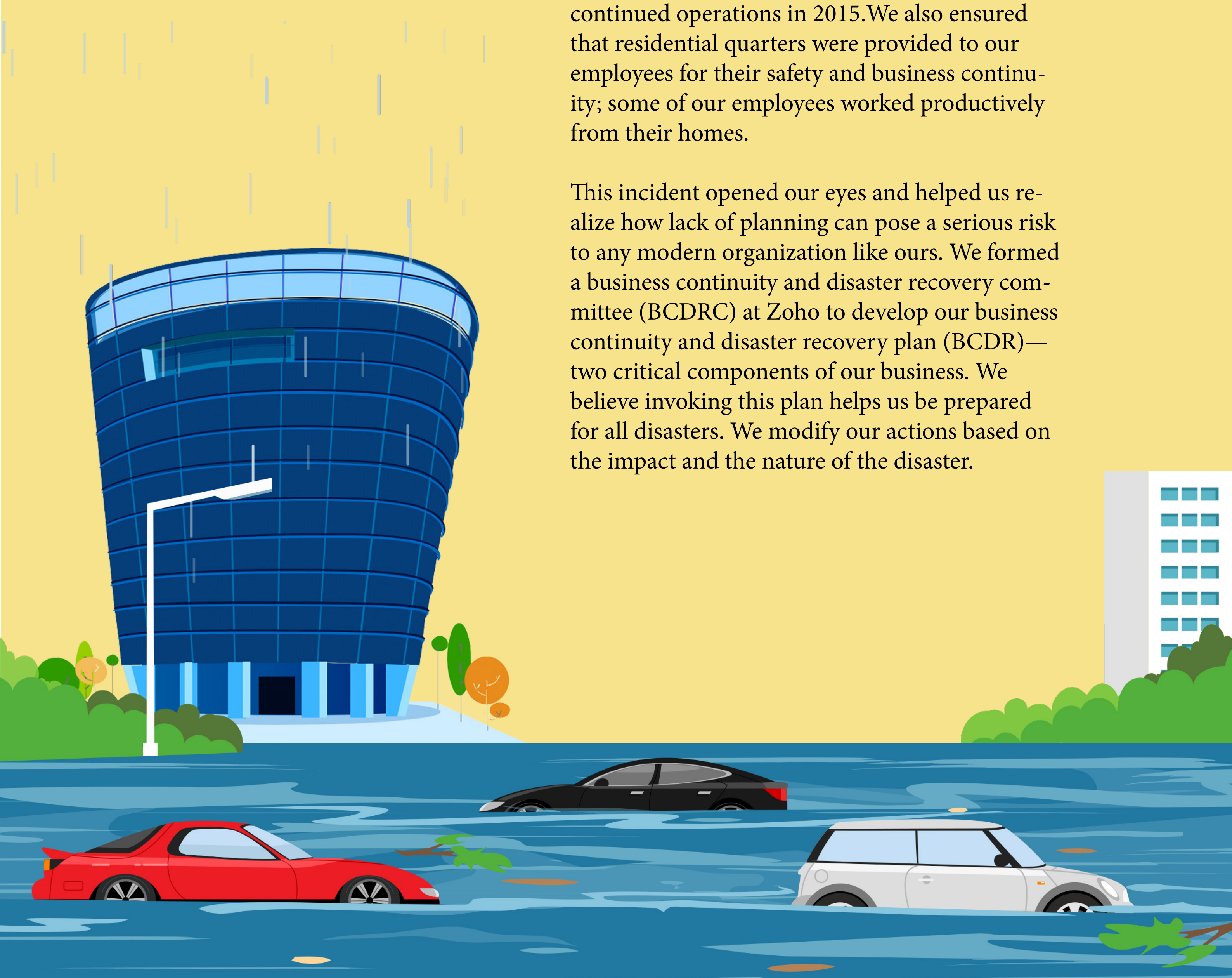


Chennai floods in 2015

In 2015, we saw the worst downpour of rains in Chennai (1,049 mm, the highest amount recorded since November 1918), followed by unprecedented flooding that left thousands of stranded citizens making their way through waist-deep water. The rains battered Chennai for a month.

We were better prepared to address the ravaging water and its damaging effects in 2015. The Estancia Tower building was completely evacuated, and operations were shut for a few days due to some of the floors being waterlogged, resulting in considerable water damage as well as broken glass. We invoked a recovery effort and some of our essential customer facing teams were moved to our offices in Tenkasi, Tamil Nadu and Bangalore, Karnataka, the alternate locations for continued operations in 2015.We also ensured that residential quarters were provided to our employees for their safety and business continuity; some of our employees worked productively from their homes.

This incident opened our eyes and helped us realize how lack of planning can pose a serious risk to any modern organization like ours. We formed a business continuity and disaster recovery committee (BCDRC) at Zoho to develop our business continuity and disaster recovery plan (BCDR)—two critical components of our business. We believe invoking this plan helps us be prepared for all disasters. We modify our actions based on the impact and the nature of the disaster.



15 years after the tsunami..

How has zohocorp evolved as an enterprise in business continuity, resilience, & response?

Our BCDR Journey

Why BCDR?

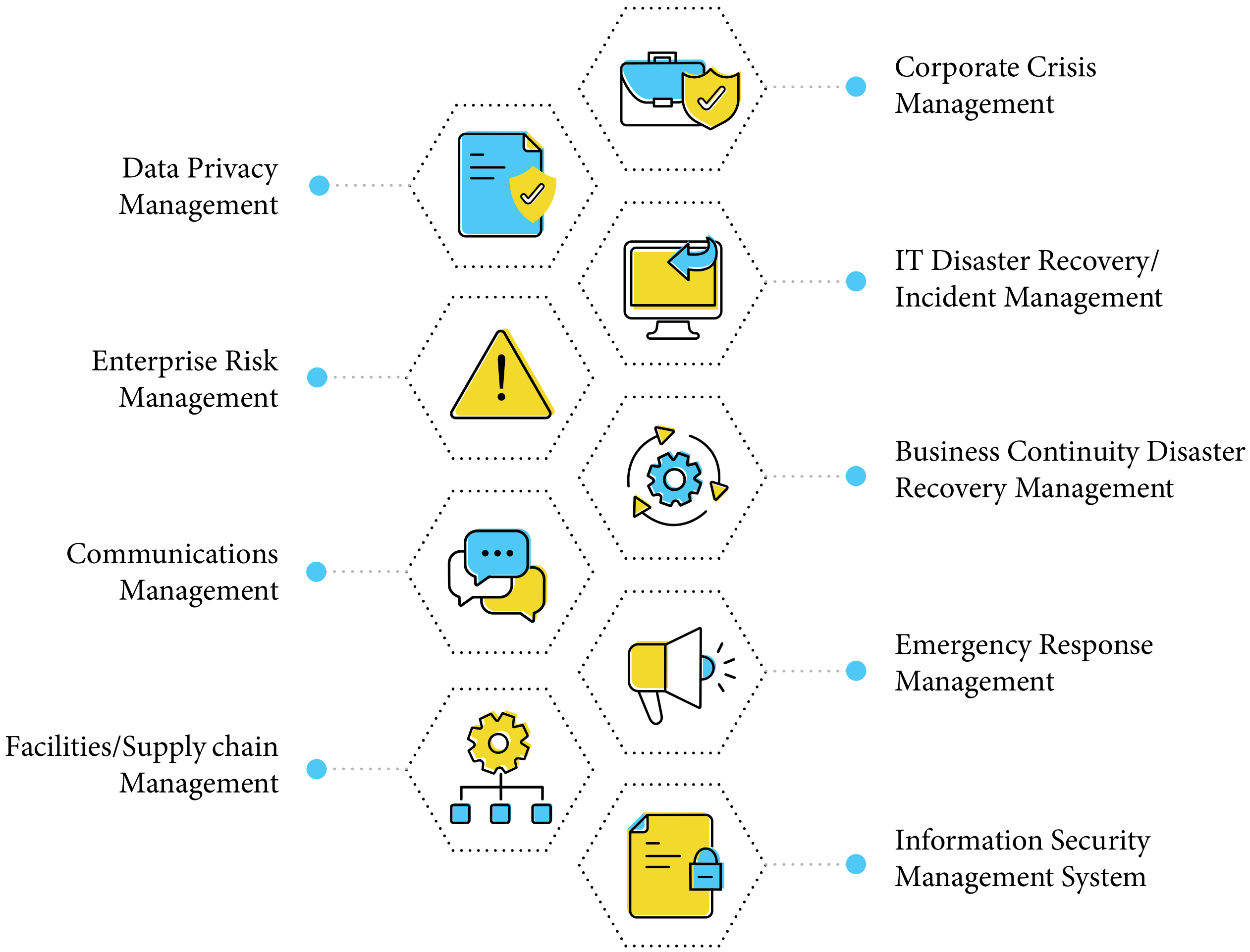
The biggest test for an organization's reputation is its ability to handle a crisis. We find that not all crises are equal. Their intensity and longevity can differ and, therefore, there is no one formula to handle a crisis.

The key to emerging unscathed is to prepare. To this end, we have a broad crisis management umbrella to determine an appropriate response for every type of crisis. Our crisis management and business continuity efforts, steered by our BCDRC, integrates the disciplines of corporate crisis management, emergency response management, incident management/IT disaster recovery (technology continuity), business continuity management, (organizational/ operational), information security management,

BCDR is its own discipline, so we should treat it that way. BCDR and preparedness have to reach down to the grassroots level, and be considered one of the mainstream processes in conjuction with continual improvement.

- Rajesh Ganesan
Vice president, Manageengine

Crisis management framework


Corporate Crisis Management
Data Privacy Management
IT Disaster Recovery/ Incident Management
Enterprise Risk Management
Business Continuity Disaster Recovery Management
Communications Management
Emergency Response Management
Facilities/Supply chain Management
Information Security Management System

In recent decades, natural disasters have become more common and costly, underscoring the need for business continuity plans to be ready to be deployed in the event of a disaster. As an enterprise, Zoho fully understands that our BCDR is vital to help our organization avoid and mitigate the risks associated with any disruptions of operations.

A disaster can impact organizations differently–a hurricane might tear the roof off one organization's building, flood another, and leave a third with no damage. While some natural disasters, such as a hurricane, can cause loss of life or significant injuries, other disasters, such as a major IT incident, might seem less dramatic but can significantly impact business operations. At Zoho, we believe preparedness is key to handling every type of disaster effectively and to ensure business continuity. (If you are running a business, then you should believe in preparedness too!)

Our BCDR records an enterprise-wide, process-oriented approach that covers the operational abilities of our data centers, IT operations, systems, customer service functions, and communication strategies. These are all critical to Zoho's resilience and successful operations, even during unforeseen circumstances.

The BCDR plan is built on these guiding principles:

Principles	Rationale
Integrate mainstream business processes	Ensure BCDR and risk management are an integral part of mainstream processes.
Gather the best and most reliable information.	Collect information from various data sources: • Internal: Stakeholders and board of directors provide evidence-based decisions. • External: Governing bodies and law enforcement
Take a people-first approach.	• Ensure the safety of our workforce.
Ensure a swift and speedy recovery.	• Operate efficiently during emergencies, and ensure that our products and services are not disrupted for our customers. • Delivery an immediate and effective response to maintain credibility in the eyes of our customers, partners, and stakeholders.
Prepare effectively to handle all types of disasters.	• Ensure our BCDR addresses the business disruption resulting from various kinds of disasters. (Refer to the section below to understand the disaster categories).
Continuously improve.	• Record the learnings from disruptive events to identify gaps in the BCDR, so we can better prepare to respond to future events.

So, should organizations start with BCDR right away?

The answer is a resounding YES. No business is immune to disasters. The history of continuity planning is riddled with examples of enterprises going out of business after a disaster. More enterprises are now shifting their focus on business continuity, understanding that downtime, especially if it lasts for a long time, can result in substantial risks and costs to their organization.

MEASURABLE	INTANGIBLE
Deferred or lost revenue	Damage to credibility and reputation
Rise in customer churn; customer dissatisfaction	Loss of goodwill with partners and customers
Less employee productivity	Loss of employee morale, and loss of trust in the organization
Penalties due to non-compliance of service-level agreements (SLAs)	Loss of competitive advantages

A comprehensive BCDR is key to dealing with unforeseen events and the resulting downtime, enabling organizations to eliminate points of failure, ensure backup plans, and restore operations quickly. However, while some enterprises struggle to develop and execute a plan, others express a myriad of excuses to avoid developing one:

“Our people will know what to do during an emergency.”

What will your employees do when something happens to your physical location? Yes, we hire the smartest and most intuitive people, but letting employees respond and act on their own will only add to the existing chaos. A well-documented business continuity plan, relevant policies, and training with live simulations can ensure that the workforce is prepared for disasters, and keeps them focused on staying as productive as possible.

“It won’t happen to us.”

We appreciate the optimism. However, it is always best to expect the unexpected as the lack of sufficient backups, disaster recovery plans, or continuity efforts can leave any business crippled, should the worst happen.

“We have insurance. We’ve got this covered!”

We’ve been in business for more than 20 years and have taken some hits along the way. That’s how we know that although insurance is part of a business continuity strategy, it cannot cover the peripheral and intangible damages resulting from an event like loss of customers, market share, or setbacks in the development of a new product.

“It isn’t our priority. We don’t have time for it.”

It happened to us; we hardly saw continuity as a priority until it became a dire requirement. In the event of a disaster, business continuity has been the key factor in keeping our business afloat. We believe that the ability to serve customers during and immediately after an event can improve credibility with the customers and ensure sustenance.

“BCDR is for large enterprises. We can relax.”

Many small-to-medium sized businesses (SMBs) believe they are too small, and having a BCDR in place can be an overkill. Unfortunately, the impact on startups and SMBs is more brutal during disasters as they typically have less cash reserves for managing sudden slumps. Having a BCDR can prevent small businesses from incurring more losses allowing them to break-even until the situation is stabilized.

Why our framework?

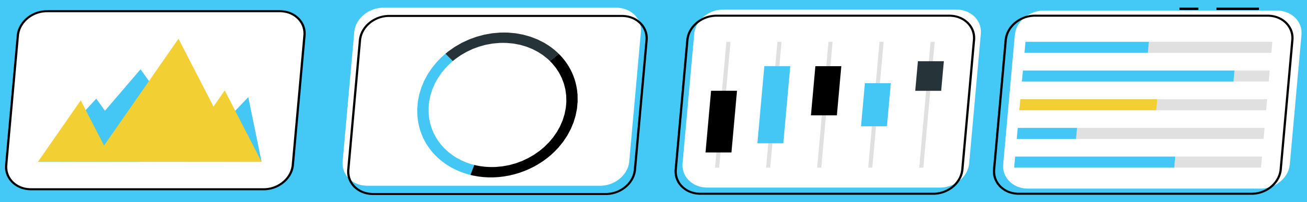
We are a Software as a Service (SaaS) provider with over 20 years of experience in software development, and with 12 offices around the world and 10 data centers. Our U.S. headquarters is currently in Pleasanton, California. The research and development campus and global headquarters is at Estancia IT Park, Chennai, India with a world-class infrastructure that hosts a workforce of nearly 10,000 individuals working on developing game-changing software products. Around 50 million customers worldwide rely on our applications for their business and IT needs.

The upcoming framework features Zoho's business continuity and disaster recovery model that includes resources, actions, processes, checklists, best practices, and information. It was created, tested, and designed to be resilient to help us avoid disruption of operations in the face of an event.

This model has helped Zoho to minimize the impact, maintain essential functions, and return to normal operations as quickly as possible followingany disaster scenario, regardless of the cause and duration. It records our learnings over the last decade, and can serve as a blueprint to simplify, and de-mystify the disaster recovery and business continuity processes for all IT organizations to develop their own BCDR efforts based on their business model.

It combines the expertise of Zoho's Business Continuity Disaster Recovery Committee (BCDRC) which includes the board of directors and senior management, making it an essential read for business continuity teams, IT managers, risk managers, auditors, and IT leaders.

If this piques your interest, then move on to our BCDR framework below.



A blueprint to keep your business running during disaster

Resilience . Recovery . Contingency

Chapter 02

A BCDR blueprint for enterprises

Zoho’s BCDR framework

Purpose and scope

- Defining purpose and scope
- BCDR governance
- Roles and responsibilites

Risk Assessment

- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment

Business impact analysis

- Conduct BIA interviews
- Create BIA report
- BCDRC approval

BCDR planning

- Disaster recovery procedures
- Business continuity procedures
- BCDRC approval

Implementation and training

- Training and education
- BCDR documentation

Continual improvement

- Plan review and maintenance

Purpose

The BCDR plan lays out the steps and procedures that Zoho and ManageEngine will follow before, during, and in the wake of a disasters, e.g., natural disasters, man-made events, pandemics, etc. We are resilient as a company, and we are committed to ensuring maximum functionality during any emergency, and returning our operations to normal in the shortest possible time.

Key elements of the BCDR:

- **Resilience:** Withstanding business interruptions in the face of adverse conditions
- **Recovery:** Returning to business as quickly as possible after a disaster
- **Contingency:** Having a comprehensive set of measures and controls in place for a full recovery
- **Continual improvement:** Continually reviewing the plan, making necessary revisions, and keeping the plan updated

Scope

The effectiveness of a BCDR depends on a well-defined scope. As Zoho is a large enterprise and has distributed teams, this process is understandably complex. There are many questions that we ask, answer, and record when determining the scope for a BCDR:

- Will it cover all work sites, disaster prone sites, or the production center?
- Will it cover all customers, or just a percentage of them?
- Will it cover a local disaster, or widespread disasters, such as hurricanes and pandemics?
- What are our essential products and services?
- What are the critical processes and business units that MUST function in the event of a disaster? Example: Customer facing teams.

Next, we validate certain assumptions. For example: skilled resources, team leaders, or alternates will be available following a disaster.

BCDR governance

Many organizations tasked with developing a BCDRimmediately start to write a plan. However, experience tells us that a good governance structure is key to steering our BCDR creation efforts, and to ensure there are no dead ends and pitfalls in the processes.

We have a control or governance system, BCDRC, that is comprised of our board of directors and senior management executives of Zoho and ManageEngine. The BCDRC is brought on board early to steer our BCDR efforts and also to ensure that,a) the right individuals are in the right roles to maximize our business continuity efforts, andb) the BCDR is kept ready and relevant at all times.

The following table highlights the roles and responsibilities of our BCDRC.

The roles and responsibilities of our BCDRC

BOARD OF DIRECTORS	SENIOR MANAGEMENT
Understand and communicate the value of the BCDR and the risks in the absence of a BCDR	Senior management team has a sound working knowledge of BCDR practices and business risks.
Review the organization's BCDR annually.	Keep the board of directors and C-suite executives informed of any significant changes to the business continuity plans.
Get frequent updates from the senior management team for any new business continuity policies and procedures.	Define Zoho's business management objectives, provide strategic inputs for BCDR, and designate the Business continuity coordinators (BCCs).
Direct and approve the planning, implementation, testing, and other strategic objectives of the BCDR.	Review and approve, during creation and when updating critical processes, the standard operating procedures (SOP) and planning exercises of our BCDR for all business units.
Direct the audit committee to prepare for external audits.	Support and communicate the importance of BCDR planning, training, and testing to all stakeholders.
Direct the external communication plan to investors, customers, the media, and law enforcement authorities.	Assign the appropriate middle managers to perform key BCDR-related procedures and exercises.

Other roles and responsibilities

WHO?	DOES WHAT?
Business continuity coordinators (BCC) are similar to incident coordinators (refer IM process here). The BCC create and maintain the BCDR and work closely with other critical business functions to understand their processes, identify risks, and also help manage and minimize those risks.	• Manage, communicate, and control all activities associated with the BCDR and the recovery of critical business functions. • Activate BCDR for affected departments. • Keep the incident manager informed of continuity/disaster recovery efforts (refer IM process here). • Meet middle management to review and prioritize critical processes of their respective business units. • Receive updates from middle managers and adjust plans as necessary. • Work with communications team and provide inputs to help craft the communications plan. • When business returns to normal, receive feedback from middle management to identify gaps, and record the learnings to continually improve the BCDR. • Maintain documentation of BCDR while ensuring confidentiality and privacy.
Middle management (Business owners)	• Interview with the BCC to determine the critical processes of their business units. • Assess risks specific to their business units. • Recommend steps to the BCDRC to address the identified risks related to their individual business units. • Collaborate with the IT management team and the BCC to design and implement BCDR based on risk assessment and the BIA.

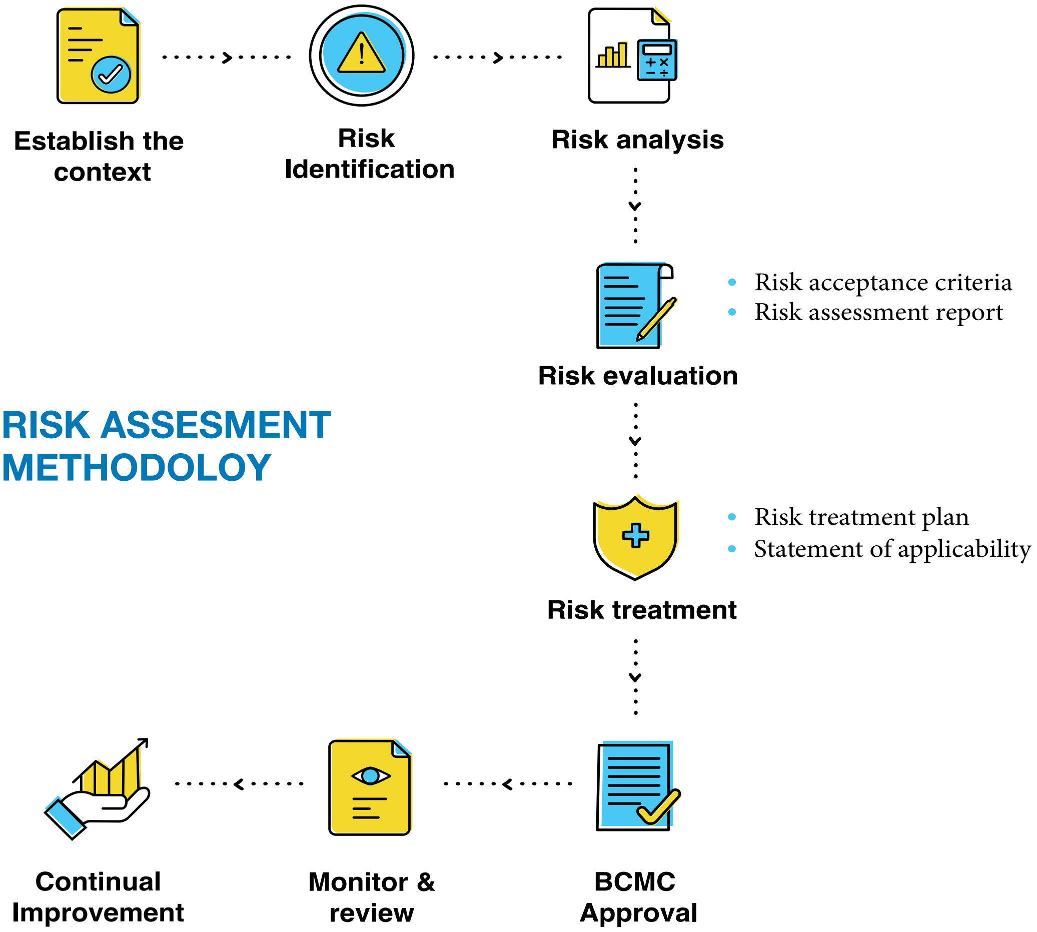
Other roles and responsibilities

WHO?	DOES WHAT?
Middle management (Business owners)	• Conduct adequate tests to ensure the correctness of the business operability procedures as per BCDR.
Audit and risk management committee (ARMC)	• Conduct internal compliance audits. • Review and report to the BCDRC on the effectiveness of BCDR.
Risk management team	• Risk owners are ultimately accountable for ensuring the risk is managed appropriately.
Legal counsel	• Identify legal risks and provide advice to BCDRC. • Supervise any internal investigations during emergencies. • Take proactive compliance measures for Zoho. • Work with spokespersons/ communications team to craft our external communication.
Other stakeholders	• Report their concerns in risk assessment and the BIA of their respective business units. • Familiarize themselves with the BCDR and emergency contacts. • Participate in testing and training sessions and provide feedback to middle management.

Risk assessment

The first and key step of BCDR is the assessment of risks. Risk is the uncertainty of achieving the objectives, which affects our business in an adverse way. Risks are realized when:

- The objectives of the business is not achieved.
- There is non-compliance with organization's policies and procedures, or external legislation and regulation.
- The resources of the business are not utilized in an efficient and effective manner.
- There is a violation of the Confidentiality, Integrity and Availability (CIA) of information.



It is important for Zoho to have an all-hazards approach to risk assessment and control processes in place to ensure that potential impacts do not become real, or if they do, there is a contingency plan in place to deal with them. It is also important that the process is clear so that successive assessments produce consistent, valid, and comparable results, even when carried out by different people.

Establish the context

The scope of risk assessment is defined based on factors such as:

- Geographical location: Distributed data centers and office set up
- Business units or departments Business process(es)
- IT services, systems, and networks
- Customers, partners, products, or services

The overall environment in which the risk assessment is carried out should be identified and rationalized. This will include a description of the internal and external context and any recent changes that affect the likelihood and impact of risks in general.

INTERNAL CONTEXT	EXTERNAL CONTEXT
Governance, organizational structure, roles and accountabilities	The cultural, social, political, legal and regulatory environments
Policies, objectives, and the strategies	Financial, technological, economic, nature and competitive environments
Capital, time, people, processes, systems and technologies	International, national, regional or local environments
Information systems, information flows and decision-making processes	Key drivers and trends which have impact on the objectives of the organization
Relatonships with, and perceptions and values of, internal stakeholders	Relationships with, and perceptions and values of, external stakeholders
The organization's culture	
Standards, guidelines and models adopted by the organization	
Form and extent of contractual relationships	
The type(s) of cloud services provided	

Risk identification

Although there are myriad disasters, the resulting effects are similar for most, and it is these we plan for. They result in scenarios such as loss of infrastructure or sustained IT failure. Preparing for the worst-case scenario helps cover many scenarios and risks in a single plan.

Our risk assessment team identifies, classifies, and assesses a wide range of disasters, especially those with catastrophically high impact potential, then characterizes their effects on business to enhance preparedness, response, and resilience.

Natural		Willful	Accidental
Sub category			
Geophysical	Earthquake	Bomb threat	Chemical spill
	Volcanic eruption	Terrorist activity	Radiation contamination
	Landslide	Civil disorder	Heating systems or air conditioning failure
	Rockfall	Bomb explosion	Telecommunications failure
Meteorological	Thunderstorm	Bio weapons	Network failure
	Lightning snowstorm	Disastrous waste	Gas leak
	Blizzard	Employee strike	Fire (internal)
	Tornado	Cyber attack	Wildfire (external)
Hydrological	Flood	Disgruntled employees sabotage an organization's systems	
	Tsunami		
	Avalanche		
Climatological	Drought		
	Heatwave/coldwave		
	Forest/land fires		
Biological	Epidemic		
	Pandemic		

Most enterprises have resilience plans for geophysical, willful, and accidental disasters, and for IT disaster recovery. These plans that are effective for various business disruptions can fall short during a global pandemic like the COVID-19.

It's important that enterprises understand the significant differences between natural disasters versus pandemic outbreaks so they can look beyond traditional business continuity strategies. At Zoho, we have established pandemic-specific policies and communication strategies to minimize business disruptions.

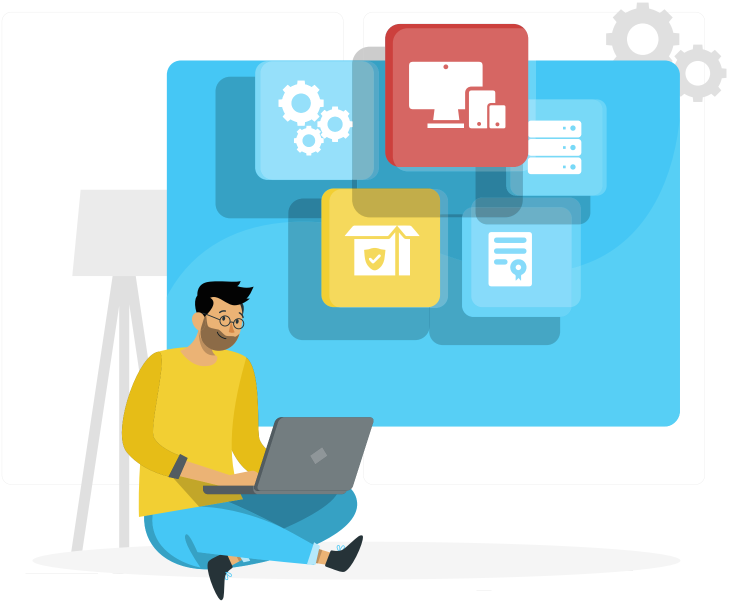
While natural disasters with physical phenomena are limited to a particular geography, biological disasters, such as viral pandemics, spread globally. The table below lists the differences between the disruptions due to natural disasters and pandemics.

Disruption differences between natural and biological disasters

Distinguishing factors	Natural	Biological
Impact	Affects the organization, facility, workforce and third parties.	A systemic event that affects everyone globally, including the organization and its workforce, customers, suppliers, and competitors.
Exposure	Can be contained and isolated as soon as the root cause is identified.	A contagion that spreads rapidly across geographies with severe impacts.
Duration	Shorter duration. Varies from a few hours to a week.	Longer duration. A viral pandemic can last for several months.
Workforce	Temporary shortage and relocating of workforce.	Significant shortage of workforce that needs other alternatives like telecommuting.
External communication	Emergencies should be reported to the appropriate law enforcement authorities, and health care assistance (e.g. police department, fire department, ambulance service).	High degree of coordination with the local government, law enforcement, health care assistance.
Infrastructure	Affects public infrastructure availability, like electricity, telecommunications, and internet.	Affects the global supply chain.

Compile/maintain asset inventory:

The definition of an asset is "anything that has value to the organization" and needs to be protected. A full inventory of assets is compiled and maintained by Zoho using the ServiceDesk Plus application. This includes customer data that Zoho stores and processes in its role as a cloud service provider.



Two major types of assets are identified as:

- Primary assets — information and business processes and activities
- Supporting assets — hardware, software, network, personnel, site, and organization structure

The list of assets is held in the document Information Asset Inventory, and in the ServiceDesk Plus application. Within the inventory, every asset is assigned a value which should be considered as part of impact assessment stage of this process. Each asset also has an owner who should be involved in the risk assessment for that asset. Where it is appropriate for the purposes of risk assessment, cloud customer data assets may be owned by an internal role and the customer consulted regarding the value of those assets. For the purposes of risk assessment, it is recommended to group assets with similar requirements so that the number of risks to be assessed remains manageable.

For each asset (or asset group), the threats that could be reasonably expected to apply will be identified. These will vary according to the type of asset and could be accidental events, such as fire, flood, vehicle impact, or malicious attacks such as viruses, theft, or sabotage. Threats will apply to one or more of the Confidentiality, Integrity, and Availability (CIA) of the asset.

Risk scenarios:

The identification of risk scenarios is performed by a combination of group discussions and interviews with interested parties such as:

- Business unit manager(s) responsible for each business-critical activity
- Representatives of the people who normally conduct each aspect of the activity
- Providers of the inputs to the activity
- Recipients of the outputs of the activity
- Appropriate third parties with relevant knowledge
- Representatives of those providing supporting services and resources to the activity
- Any other party that is felt to provide useful input to the risk identification process

The identified risks along with a description are recorded to assess the likelihood and impact of the risks.

Disasters and risk scenarios identified in the last decade

HAZARDS	RISK SCENARIOS
Earthquakes Floods Tsunami Pandemic Ransomware DDos attacks Telecommunication failure Network failure	Irreversible damage to IT infrastructure Half of core revenue generating business units Loss of Zoho production center (Zoho Estancia building) & data centers Loss of critical customer data Absenteeism of critical employees Loss of access to our worl sites Interruption of supply chain

Risk analysis

This process involves assigning a numerical value to the a) likelihood and b) impact of a disaster. These values are then multiplied to arrive at a classification level of high, medium, or low for the disaster.

Assessing the likelihood:

An estimate of the likelihood of a disaster occurring is made. This should take

into account whether the disaster has occurred before either to Zoho or to similar organizations, or at the location and whether there exists sufficient motive, opportunity, and capability for a threat to be realized.

The likelihood of each disaster is graded on a numerical scale of 0 (low) to 3 (high). When assessing the likelihood of a disaster, existing controls are taken into account, and that means an assessment has to be made on the effectiveness of existing controls. The rationale for recording assigned grades to a disaster risk is to aid understanding and to help with future assessments.

LIKELIHOOD		
PROBABILITY	**EXPLANATION**	**SCORE**
LOW	An event that never occured	**0**
	An event that is highly unlikely to occur of occurs rarely (perhaps once in 3 years)	**1**
MEDIUM	An event likely to occur relatively infrequently, perhaps once a year	**2**
HIGH	An event that is fairly probable, and could be expected to occur several times a year	**3**

Assessing the impact:

An estimate of the impact that the disaster risk could affect the Confidentiality, Integrity or Availability on the organization is given. This will take into account existing controls that lessen the impact, as long as these controls are seen to be effective. Consideration will be given to the impact in the following:

- Customers
- Finance
- Health and safety
- Reputation
- The secondary, indirect, or cumulative effects within the organization
- Legal, contractual, or organizational obligations

The impact of each risk is graded on a numerical scale of 0 (low) to 3 (high).

PROBABILITY	EXPLANATION	SCORE
LOW	No impact	0
	Negligible or less impact with less effort to repair	1
	Damage to reputation or revenue loss is minimal	
MEDIUM	Tangible harm, extra effort required to repair	2
	Damage to reputation or revenue loss is significant	
HIGH	Significant expenditure of resources requires and compromise of the system	3
	Damage to reputation and revenue loss is high	

Risk classification:

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers (likelihood X impact level). This resulting score is then used to decide the classification of the risk based on the matrix

Risk formula:

RISK = LIKELIHOOD X IMPACT

Each risk will be allocated a classification based on its score as follows:

RISK VALUE	RISK LEVEL	COLOR CODING
0-3	LOW	🟩
4-6	MEDIUM	🟨
7-9	HIGH	🟥

Note: Based on our risk appetite, we do change the definition of high, medium, and low classifications. For example: We may decide that only risks with a score of 16 or more

Risk evaluation

Risk acceptance criteria:

Risk treatment will not be done for the risks which are ranked in the "Low" risk level. If the value is rated as 3, no actions are taken. If the value is rated as >= 4, the actions will be initiated. Risk treatment can still be done for the "Low" risk category, should the BCDRC decide to do so.

We evaluate risks to decide on the risks that can be accepted and the ones that need to be treated. This should take into account the risk acceptance criteria. The matrix above shows the classifications of risks, where the green indicates that the risk is below the acceptable threshold and could be regarded as "safe". The orange and red areas generally indicate that a risk does not meet the acceptance criteria and needs to be treated. Risks will be prioritized for treatment according to their score and classification so the high scoring risks are recommended to be addressed before those with lower levels of exposure for the organization.

Risk assessment report:

The results derived from risk evaluation is captured in the risk assessment report with the following information:

- Assets (asset-based risk assessment only)
- Threats
- Vulnerabilities
- Risk scenario descriptions (scenario-based risk assessment only)
- Controls currently implemented
- Controls currently implemented
- Likelihood (including rationale)
- Impact (including rationale)
- Risk score
- Risk classification
- Risk owner
- Whether the risk is recommended for acceptance or treatment
- Priority of risks for treatment

Note: The risk assessment report holds the inputs to the risk treatment stage of the process and is signed off by the BCDRC before proceeding further, particularly those risks that are recommended for acceptance.

Risk treatment

Risk treatment is a process to develop a range of options for mitigating the risks that are agreed to be unacceptable. We apply the following measures to treat the risks:

1. **Modify** the risk by applying appropriate controls to lessen the likelihood and/or impact of the risk.
2. **Avoid** the risk by taking actions that means it no longer applies.
3. **Share** the risk with another party.
   For example: insurer or supplier.

We use our judgement to decide which course of action to follow based on a sound knowledge of the circumstances surrounding the risk. Example: Business strategy, regulatory and legislative considerations, technical issues, commercial and contractual issues.

Note: The risk reviewer ensures that all parties who have an interest or bearing on the treatment of the risk are consulted, including the risk owner.

Risk treatment plan:

On evaluating the treatment options, the risk treatment plan is created with the below details:

- Risks requiring treatment
- Risk owner
- Recommended treatment option
- Control(s) to be implemented
- Responsibility for the identified actions
- Timescales for actions
- Residual risk levels after the controls have been implemented.

Statement of Applicability (SOA):

The SOA sets out those standard controls that have been selected and the reasons for their selection. It also details those that have been implemented and identify any that have been explicitly excluded along with the reasons for exclusion.

BCDRC approval

At each stage of the risk assessment process, the BCDRC is kept informed of the progress, including the formal sign off of the proposed residual risks. The BCDRC approves the following documents:

1. **Risk assessment report**
2. **Risk treatment plan**
3. **Statement of Applicability (SOA)**

The acceptance or treatment of each risk will be signed off by the relevant risk owner.

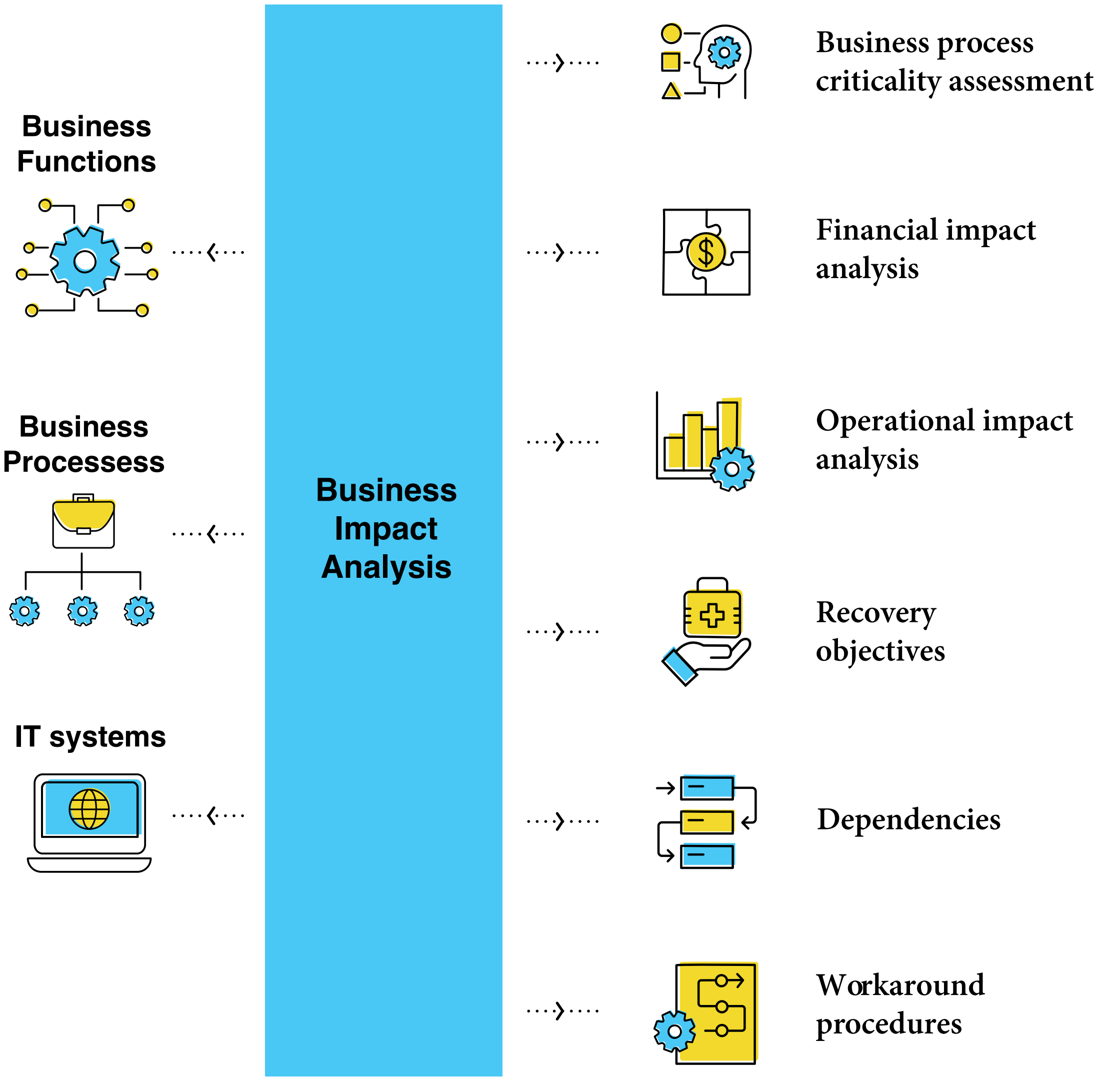
Risk monitoring & reporting

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators (KPIs) are identified which allows measuring the success of the relevant risk controls. These indicators are reported on a regular basis and trend information is produced so that exceptional situations are identified and dealt with as part of the BCDRC review process.

Regular reviews

In addition to a full annual review by ARMC, risk assessments are evaluated on a regular basis to ensure that they remain current, and the applied controls are valid and relevant. The relevant risk assessments are also reviewed upon major changes to the business such as office moves, mergers and acquisitions, or introduction of new or changed IT services.

Business impact analysis



While some business functions maybe relatively unimportant, some are absolutely critical to ongoing business. The BIA process makes it easy to pinpoint the most critical business functions, their interdependencies, and whether they should be considered for inclusion into the business continuity strategy. It also helps us identify how these core functions can be impacted by disasters, and also lays the groundwork for more systematic and logical recovery plans.

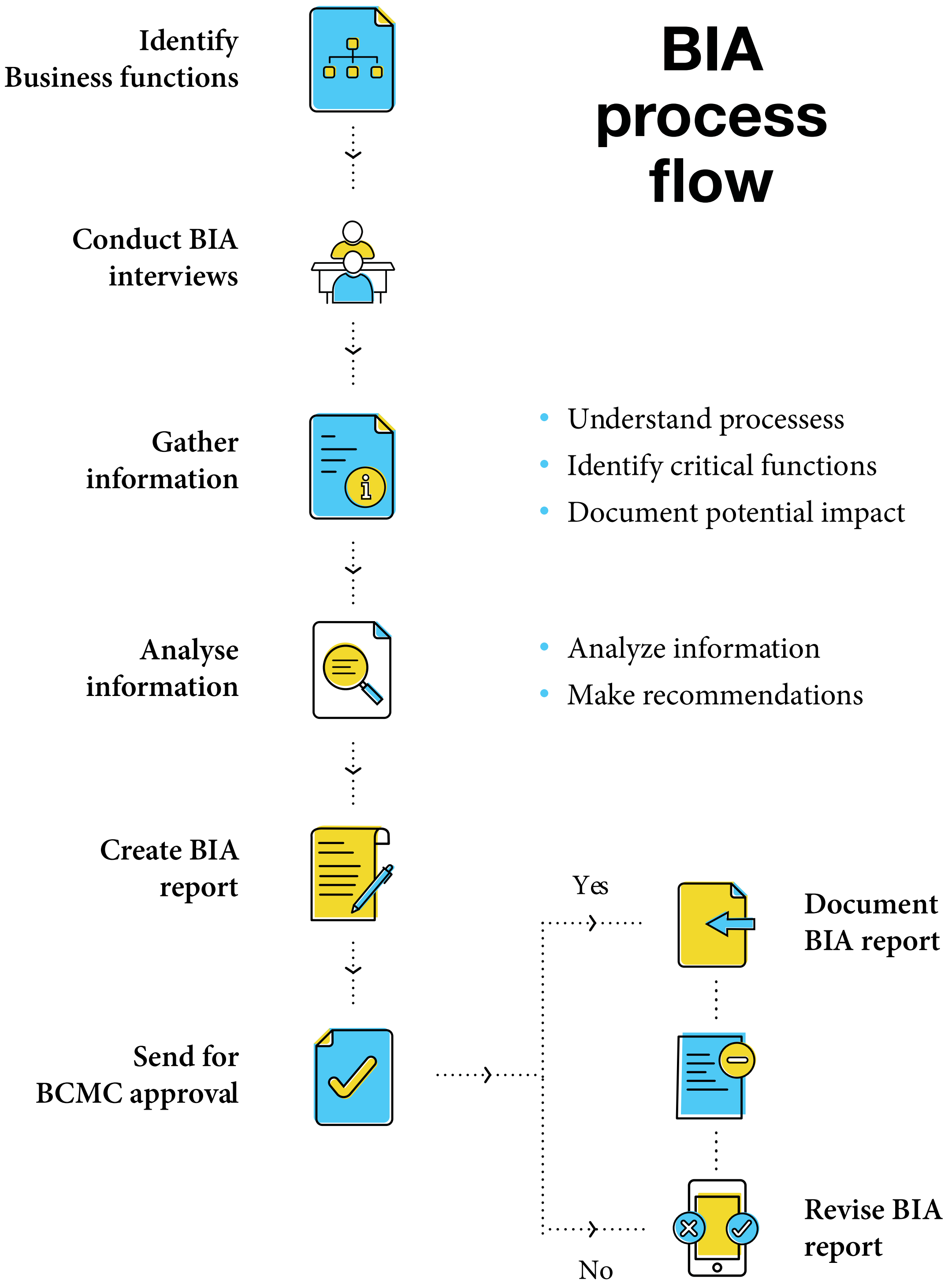
Conducting this analysis makes us more confident and secure about our business decisions, knowing that our decisions are based on a solid understanding of the most essential components of our business.

The core objectives of BIA are as follows:

- Prioritize business-critical units or departments, products, and services that must be protected.
- Create an inventory of essential business activities and the minimum resources required to conduct business at a normal or near-normal state.
- Establish recovery time frames or recovery time objectives to help prioritize risk treatment plans and select the appropriate response and recovery strategies.

As shown in the process activity diagram below, BIA is a multi-phase process performed by BCC.

BIA process flow



Identify Business functions

Conduct BIA interviews

Gather information

- Understand processess
- Identify critical functions
- Document potential impact

Analyse information

- Analyze information
- Make recommendations

Create BIA report

Send for BCMC approval

Yes

Document BIA report

No

Revise BIA report

BIA interviews

The BCC takes stock of all business units and gathers some basic information before the actual interview using a Zoho Creator form. A link with the questionnaire is sent out as an email in the name of a department head, along with a note of what the BCC are trying to accomplish through this exercise and why it's important. A reasonable amount of time (around 2 weeks) is given to the teams assigned to complete the task. This prework sets the stage for a more focused and effective BIA interviews and also cuts down the time.

The BCC initially asks the below questions:

- Name of the business unit?
- What the business unit does?
- How many resources does the business unit have?
- Where is the business unit located?
- What are the hours of operation? Does it involve shifts?

Gather information:

The BCC holds a kick off meeting to hand out the questionnaire to the department heads and to clearly articulate the purpose of the whole exercise. The questionnaire covers all the required data points as the final output of the BIA relies on this step. Below is a sample questionnaire from the BCC:

Sample questionnaire from the BCC

Data points	Questions	IT related questions
Business unit and processes	Describe your business unit and its processes?	What IT systems and applications does this business unit use?
Dependencies	What are your dependencies with other business units? Would a disruption of this business unit impact others? How and when would this disruption to other units happen?	What are the IT systems that impact or are impacted by this business unit?
Resource dependencies	Does this business unit depend on any key job functions? If yes, then what is the job function and to what extent does this business unit depend on it? What is the minimum number of resources needed for this business unit to function?	What are the secondary systems, if any, needed for these job functions?
Expertise dependencies	Does this business unit depend on the knowledge and expertise of a skilled worker? If yes, describe the role and expertise of the skilled worker and the impact on business in their absence.	
Operational	If this business unit did not function, how would it impact business?	If this business unit did not function, how would it affect IT operations?

Sample questionnaire from the BCC

Data points	Questions	IT related questions
Tolerance to outages	In the face of a disaster, such as loss of production center (Zoho Estancia), how long can the business unit/systems sustain before the loss impacts the organization, its stakeholders, and suppliers?	
Minimum infrastructure requirements	What are the infrastructure requirements for your business unit: physical space, office supplies, network, communication, furniture, lighting, HVAC, water, and food supplies?	
Others	What are the other concerns, if any, that can affect the recovery of your business unit?	
Alternate business processes and resources	What arethe work-arounds currently in place for your business processes? Which individuals are the designated alternate or backup resources?	
Critical documentation	Where do you store your critical documents? Mention the type of documents, location, and alternate locations (if any)	

Sample questionnaire from the BCC

Data points	Questions	IT related questions
Recovery timeframes	What are the potential recovery issues for your business unit? What is the minimum recovery time frame? Which individuals are the essential resources needed to restore operations to a near-normal state?	
Financial impact	If this business unit did not function, what would be the financial impact on business? When would the impact be realized? Will it be a one-off impact or recurring?	
Recovery timeframe	What is the minimum time frame (in hours, days, weeks, months) required to recover for this business unit?	How long would it take to recover or replace the IT systems/ applications related to this business unit?
Service-level agreements (SLAs)	Are there any SLAs in place for this business unit? In the event of a disaster, what would be the impacton the SLAs? What are the key metrics associated with the SLAs?	How is IT impacted during disruption of this business unit?
IT applications	What software applications are needed for this business unit?	What IT assets are needed to run these applications and to support this business unit?
Desktops, laptops, workstations	How many desktops, laptops, workstations are needed for this business unit?	What is the configuration data for these systems?
Servers and networks	Does this business unit require backend systems and network?	

Sample questionnaire from the BCC

Data points	Questions	IT related questions
Work-arounds	Does this business unit have any work-around processes that have been developed and tested? If yes, would these processes facilitate the smooth function of this business unit during an event? If no, is it feasible to develop such work-arounds?	Are there any IT-related work-arounds for this business unit? If yes, what are those work-arounds and how can they be implemented?
Remote	Will this business unit be able to work from the Zoho backup recovery sites? Or, could members of the business unit work remotely from home?	What should IT do to enable remote access for this business unit?
Vital records	Where does this business unit store critical documents? Are these documents backed up? If yes, where and how frequently does the business unit backup documents?	Where are the document backups stored? Is the current document backup strategy sound enough?
Previous business disruption experience	Has this business unit faced any disruptions earlier? If yes, what was the disruption scenario and duration? Are there any learnings that can be incorporated into the BCDR to prepare for future disruptions?	Has IT been involved in this disruption scenario? If yes, how did IT address this disruption?
Competitive impact	What would be the competitive impact to Zoho if this business unit faced significant disruption? What percentage of customers would we lose?	

The BCC conducts follow-up interviews to validate the gathered information, and to fill any gaps.

Analyze the information:

The questionnaire is created to gather information about the financial and non-financial impacts, recovery timeframes, resource, and application requirements. The BCC compile and analyze the responses to provide the required information to develop a corporate-wide recovery and continuity strategies.

The table below captures some of the most important impact categories that we consider. This table can be used as a checklist by other IT organizations while conducting a BIA.

Impact categories	Natural
Financial impact	• Loss of revenue due to lost sales • Penalties due to non-compliance of SLAs • Increased operating, relief, and recovery expenses
Exposure	• Damage to production/data centers • Restricted access to work sites • Damage to IT systems • Damage to other physical assets • Loss of data • Loss of network, power, telecommunication systems • Supply chain disruption
Resource	• Absenteeism • Low employee morale
Health and safety	• Compromised employee health (pandemics) and safety worker safety (fire) • Environmental damage

Impact categories	Natural
Legal	• Inability to fulfill SLAs • Inability to comply with regulations
Strategic	• Delay in new business initiatives • Lack of innovation due to less employee engagement resulting from the disruption.
Intangible	• Dissatisfied customers • Customer defection • Damage to Zoho's business reputation • Loss of goodwill with partners • Loss of employee morale

The information gathered in the BIA interviews is used to:

- Identify the critical business units and processes
- Define the recovery time objective (RTO) for each business process.
- Define the recovery point objective (RPO) for each business process
- Identify resource requirements

Identifying critical functions:

In the big picture, how critical is each business unit and their processes to Zoho's ability to operate? A three point rating system helps the BCC assign a "criticality rating" to a business unit and its functions.

CATEGORIES	CRITICALITY	COLOR CODING
1	**Critical** (mission critical BUs and processes)	🟥
2	**Important** (necessary BUs and processes)	🟧
3	**Minor** (Desirable BUs and processes)	🟦

Category 1:

Critical business units and processes are those that are:

- most sensitive to downtime,
- maintain cash flow,
- fulfill SLAs, and
- play a key role in maintaining Zoho's business reputation.

The BCDR focuses more time and resources on the critical business units and functions first, followed by the important business units and functions.

Category 2:

Zoho's business operations in the short term aren't typically impacted by non-functioning business units and process. However, if the situation continues into the long term, non-functioning business units and processes can disrupt operations.

Category 3:

Minor or desirable business units and processes do not cause significant business disruption to business. Their impacts are usually addressed in the later stages of business recovery.

Recovery time objective (RTO)

Once the impact data is analyzed, the BCC define the RTO, which is the time a business process should be restored following a disruption. This depends on the criticality of a business unit, process, and application and range anywhere between no downtime to several days or weeks. Simply put, "How long can we be down?"

This time frame can vary by organization — for some IT organizations, the recovery time for processes can be as low as 0 minutes.

CATEGORIES	CRITICALITY	COLOR CODING
1	**Critical** (mission critical BUs and processes)	**12 hours or less**
2	**Important** (necessary BUs and processes)	**48 hours or less**
3	**Minor** (Desirable BUs and processes)	< 3days

Recovery point objective (RPO):

RPO defines the maximum acceptable data loss that can be tolerated by a critical business process. Simply put, if the IT systems supporting a critical business process were to fail, how much data can be recovered? We use three time frames here and this can also vary by organization.

RPO 0 — no data loss (real time backups)
RPO 1 — less than 4 hours data loss
RPO 2 — 24 hours data loss

Identifying resource requirements and dependencies:

The BCC document each department and process along with the resource(s) responsible for the processes of a business unit. A list of backup resources for the process is also identified in case the lead resources are unavailable during an emergency.

The BCC also identifies the systems, applications (be it a CRM, payroll, or HR software), and the level of access needed to get their jobs done. The level of reliance of a business unit on these systems and applications is rated as high, medium, or low in order to ensure the availability of crucial systems and application during an emergency.

A thorough understanding of interdependencies between business units, their functions, and IT systems is crucial to both disaster recovery and business continuity. If System A is down during an event, it's pointless for our IT teams to spend a week trying to restore System B while System A is nonfunctional. The BCC document and highlight these interdependencies at this stage to ensure the effectiveness of business continuity.

BIA Report

Outcomes from the BIA are documented with recommendations of recovery strategies and presented to the BCDRC for approval. The BIA report is also appropriately incorporated into our IT disaster recovery and incident management plans. Here is a sample BIA report of one of our business units, network operations.

Business unit info:

Business unit name: Network operations center (NOC)
Business unit head: Prabhu Ponnukumaraswamy
Email ID: xxxx@zohocorp.com
Mobile: +919999999999

Headcount

50

Priority

Critical

Priority

- Critical

Business unit functions

- Network monitoring.
- Incident response.
- Provide 24/7 LAN, WAN, VPN, and network connectivity with 99.999 percent uptime.
- Provide hardware and software application support to the employees.
- Manage the IT infrastructure of Zoho.

Business unit disruption impact

Disruption of the NOC will impact all business units and the productivity of Zoho directly. Disruption of this business unit means Zoho will not be unable to conduct business and the downtime will be directly proportional to lost dollars.

RTO	RPO
15 minutes.	Zero

Internal dependencies

Human Resources, Finance, Facilities, and Security.

External dependencies

- Dependency on external physical server vendors and technicians
- ISP for network connectivity

Recommendations

- Backup site should be at a safe distance from the production center. (Tenkasi)
- Safe to engage two external ISP vendors for network connectivity

BCDRC Approvals

The BIA report is sent to the BCDRC for their perspective and approval, as results from the BIA is used to formulate recovery strategies and continuity planning. The BIA goes through a multi-step approval process. The first level of approval is conducted by the BIA owner, and the final go ahead is given by the BCDRC.

BCDR planning

The bulk of our work developing our BCDR plan is complete at this point. This section is where everything comes together: the risk assessment gave us the data to help us identify the business impact of those risks. All of that data now helps us identify the disaster response, mitigation, and recovery strategies, as well as the people, resources, and activities that we need for an effective BCDR plan.

The BCDR plan includes two phases:

- Emergency response procedures that all Zoho worksites will follow as appropriate for disasters like fire, flood, and earthquakes to protect employee lives and limit damages.
- Disaster recovery and business continuity activities conducted after the disruption for the restoration of business operations.

Roles and responsibilities

One of the crucial steps in emergency response and recovery is assigning roles and responsibilities. When disasters strike, the response teams on the scene are our first line of protection.

These teams help contain the impact of the disaster and effect a timely recovery before the first responders such as police or firefighters arrive at the disaster site.

Below are the response teams and responsibilities.

BCDR	
Roles	**Responsibilities**
Emergency personnel	• Engage trained emergency personnel to act as floor wardens during the disaster, and to aid the EMT in immediate evacuation. • Notify security personnel • Brief external emergency services upon arrival on the type and location of the emergency, summarize the damage, e.g. minimal, heavy, total destruction, and the status of the evacuation • Notify building security personnel who will establish security at the facility and not allow access to the site unless notified by the BCDRC
Security personnel	• In the event of an emergency, safety and security operations are one of the first points of contact for the BCDRC • Contact the appropriate national emergency service agency • Activate evacuation alarm followed by a verbal announcement to all employees to evacuate the building • Outside of business hours, the security personnel remain on-call to notify the BCDRC and manage an emergency • Provide emergency response to all on-site emergencies • Provide security resources and work with all recovery teams as needed • Contact external emergency services
Head of facilities	• Responsible for life safety measures of employees including fire alarms, extinguishers, emergency lighting, fire detection systems, emergency exits, and other warning systems • Provides emergency floor plans on request • Ensure all employees evacuate the facilities and meet at the assigned outside location (assembly point) and follow instructions given by the emergency personnel • Acts as a liaison between Zoho and essential services vendors, such as those for HVAC, electrical, and plumbing

BCDR	
Roles	**Responsibilities**
In-house medical officers	• In-house medical officers are mobilized during emergencies
Ambulance service	• Provide transport for the injured employees
Employees	• Familiarize themselves with the standard emergency procedures • Respond to emergencies • Follow instructions from the emergency and security personnel • Keep all emergency exits clear and avoid panic during emergencies
Disaster recovery team	• Coordinate with EMT and BCDRC for appropriate recovery actions • Notify all company department heads and advise them to activate their plan(s) if applicable, based on the disaster situation • Determine recovery needs • Establish command center and assembly areas • Assess the damage to the affected location and/or assets • Provide security resources and work with all recovery teams as needed • Contact vendors/contractors of installed equipment for their expert opinions on the condition of the equipment • Document assessment results using assessment and evaluation form • Inspect the affected areas to assess damage to essential hard copies of records (files, manuals, contracts, documentation, etc.) and electronic data

BCDR	
Roles	**Responsibilities**
Disaster recovery team	• Gather information regarding damage to other work site(s), e.g. environmental conditions, physical structure integrity, furniture, and fixtures from the DRT • Develop a restoration priority list, identifying facilities, vital records, and equipment needed for resumption of activities that could be operationally restored and retrieved quickly • Prepare post-disaster debriefing report
Emergency management team	• Evaluate which recovery actions should be invoked and activate the corresponding recovery teams • Evaluate and assess damage assessment findings • Set restoration priority based on the damage assessment reports • Provide senior management with ongoing status information • Act as a communication channel to corporate teams and major customers • Work with vendors and the DRT to develop a rebuild/repair schedule
Information Technology	• Facilitate technology recovery and restoration activities, providing guidance on replacement equipment and IT systems • Coordinate removal of salvageable equipment at the disaster site(s) that may be used for alternate site operations

Notification procedures

- During standard business hours: On observation or notification of a potentially serious situation, the employee identifying the incident (termed “the reporter”) calls their business unit head. If the business unit head is unreachable or incapacitated, the reporter calls their backup, a senior manager.

- The business unit head/backup notifies the emergency personnel on site,who carry out the standard emergency and evacuation procedures if necessary,as well as the EMT and the DRT.

- Outside of business hours: The building management system (BMS) team notifies the EMT and the DRT.

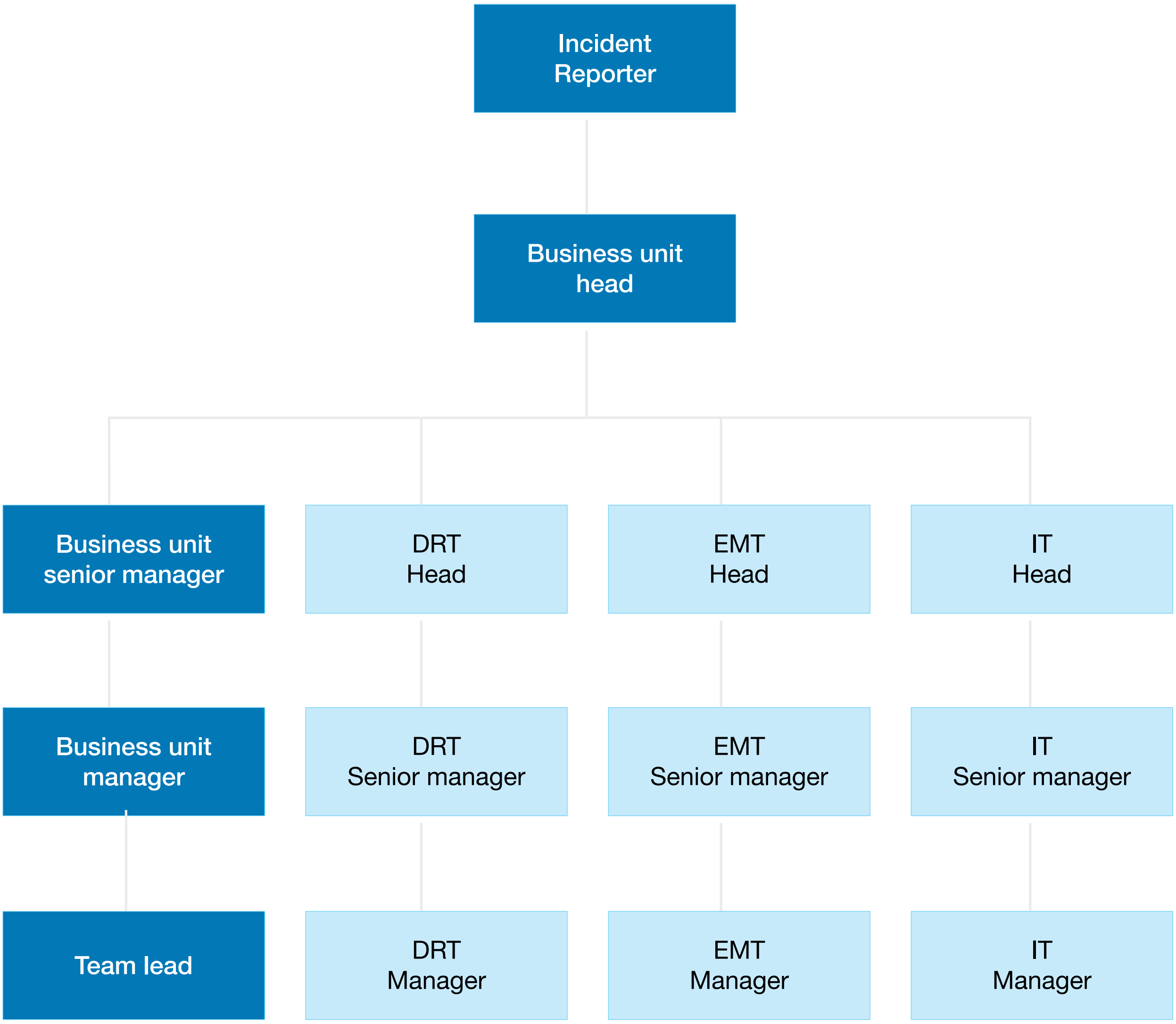
- The EMT, the DRT, and other response teams take action, based on the directives specified by BCDRC.

- When a disaster is declared, the EMT notifies IT immediately for deployment. The DRT will step in as necessary and follow up.

- The person who is authorized to declare a disaster within the BCDRC has a backup who is also authorized to declare a disaster when necessary. For example: CEO = primary authority, COO = secondary authority.

A call tree is a general notification technique that we use to list the primary and alternate contact numbers of key personnel, as well as the backup personnel numbers if the key personnel is unreachable. The contact list includes the name, department, role, mobile number, residential number, and address of the key and backup personnel.

What’s at stake for Zoho



Disaster declaration:

A disaster is declared only when the emergency is not likely to be contained and resolved within predefined time frames. The BCDRC is responsible for declaring a disaster and has to be well informed about the geographical, political, social, and environmental events that can pose a threat to Zoho’s business operations. To avoid false alarms, the BCDRC has identified institutions that provide timely and meaningful disaster predictions that allows Zoho to respond and recover effectively. Below are a few identified institutions that help the BCDRC with disaster monitoring for regional work sites.

Type of disaster	Early warning/prediction systems (For regional work sites)
Cyclones and earthquakes	Indian meteorological department and earthquake sensors
Tsunami	Indian national centre for oceanic information services
Floods	Central water commission

Invoking the plan

Like every IT organization, we hope to never have to invoke the BCDR. However, emergencies can arise at any time and we believe in readiness. The BCDR is reserved for significant disasters and business disruption and is invoked by BCDRC.

Regardless of the service disruption circumstances, or the identity of the individual(s) in the BCDRC who are first notified of the disaster, the EMT and DRT are activated immediately in the following cases:

- The production center at Estancia is down due to a natural disaster like flood, earthquake etc.
- Any disruption in the IT systems or network facility that can cause concurrent downtime in the production center for more than three hours.

Internal communication:

Effective internal communication is key to ensuring that employees are well-informed, supported, reassured, and most importantly safe during a disaster. Ideally, a face-to-face communication is effective for relaying messages to stakeholders during a disaster. At Zoho, a forum post from the CEO and HR with key messages surrounding the disaster and BCDR on Zoho Connect is an effective communications channel. Zoho Connect is a collaboration software, like an internal Facebook-like application, that connects all stakeholders and enables multi-way communications during a disaster. Alternative communication options include WhatsApp and SMS.

In addition to the forums on Zoho Connect from the BCDRC and HR teams, the business unit heads are the focal points for their departments to provide updates on the progress of their disaster recovery and business continuity efforts, and how they can contribute to the recovery efforts.

Initial response

It might sound obvious but the BCDR prioritizes our employees and their lives over assets.

The emergency response procedures taken in the initial minutes of an emergency are critical to saving the lives of our employees. Our emergency procedures capture four protective actions: evacuation, shelter, shelter-in-place, and lockdown. These emergency actions apply to all employees (including management personnel), and to all work sites of Zoho Corporation.

Authority:

The instructions and guidance given by Zoho's trained emergency personnel overrules the reporting structure. This authority is given to the emergency personnel to ensure that the life and safety of the employees takes precedence over IT systems, other assets, and production during an emergency.

Assembly points

The BCDR plan identifies two assembly points both inside and outside Zoho premises where employees should gather after evacuating. These evacuation areas have sufficient space to accommodate all of Zoho's employees, and are away from buildings, power lines, trees, gas lines, poles, and vehicles.

The BCDR plan identifies two evacuation assembly points

- Primary - Open ground behind Zoho.
- Secondary - Open ground across the street opposite of Zoho.

Protective action and emergency procedures by disaster types

DISASTER	PROTECTIVE	
TYPE	ACTION	PROCEDURES
Fire/smoke	Evacuation	1. If fire or smoke is present in the facility, evaluate the situation and determine the severity, categorize the fire as "major" or "minor" 2. In the case of minor fires (e.g. single hardware component or paper fires), the employees attempt to put out the fire with the hand-held fire extinguishers located throughout the Zoho facilities. Any other fire or smoke situation should be handled by qualified building personnel until the local fire department arrives 3. In the event of a major fire, the fire alarm system has to be activated immediately and ring continuously for 60 secs 4. The person reporting the fire has to provide the recovery teams with their name, extension, work location (block, floor, workstation ID), and the nature of the emergency. They must follow all instructions given 5. The person reporting the fire should reach the EMT and DRT on their mobile numbers 6. The emergency personnel assist employees (giving utmost care for the physically-challenged), with safely exiting the building. Elevators cannot be used 7. All employees are required to gather at the assigned outside location or assembly point, and follow instructions given by the emergency personnel 8. Following the evacuation, a headcount will be taken to ensure all individuals are accounted for 9. The assembly area has to be monitored, and employees should be reassured of their safety 10. Appropriate first aid will be given to any injured individuals by the in-house medical officers until the paramedics arrive
Flood/water damage	Evacuation	1. Cease operations and usage of electrical equipment and move to higher ground

DISASTER	PROTECTIVE	
TYPE	ACTION	PROCEDURES
Flood/water damage	Evacuation	2. If water is dripping from an air conditioning unit and is not endangering IT systems and other assets, contact plumbing and HVAC repair personnel immediately 3. If flooding is severe, activate alarm/warning system for employees and immediately notify EMT/DRT teams, emergency personnel, and implement power-down procedures 4. While power-down procedures are in progress, evacuate the area and follow BCDRC instructions 5. Evacuate the work site building if necessary and proceed to the emergency assembly area. Follow evacuation procedures 6. The DRT call the national emergency number immediately and wait for outside help
Tornado/ cyclones	Shelter	1. Activate the alarm system to warn employees 2. Notify the EMT/DRT teams 3. Follow instructions from emergency personnel, and move to the basement, lower floors, and the strongest side of the building 4. If there is no basement, go to a hall/room on the lowest level of the building 5. Move away from glass windows, large shelves, ceiling decor, and other potentially harmful objects 6. A power failure might occur. Stock supplies, such as water, nonperishable food, first-aid, batteries, flashlights, and other necessities based on the forecasted duration of the tornado or cyclone 7. Employees are required to remain inside campus until the cyclone or tornado passes 8. Heads of the business units must take a headcount and notify emergency personnel in case of missing individuals

DISASTER	PROTECTIVE	
TYPE	ACTION	PROCEDURES
Earthquakes	Shelter-in-place	1. Cease operations and use of electrical equipment, and move to higher ground 2. If water is dripping from an air conditioning unit and is not endangering IT systems and other assets, contact plumbing and HVAC repair personnel immediately 3. If flooding is severe, activate alarm/warning system for employees and immediately notify EMT/DRT teams, emergency personnel, and implement power-down procedures 4. While power-down procedures are in progress, evacuate the area and follow BCDRC instructions 5. Evacuate the work site building if necessary, and proceed to the emergency assembly area. Follow evacuation procedures 6. The DRT call the national emergency number immediately and wait for outside help
Terrorist attack	Lockdown	1. When a terrorist attack is suspected and gun shots are heard, the primary evacuation route is not safe. All employees, including emergency personnel, should find safe spots to hide and remain silent 2. Mobile devices are to silenced by turning off both the ring tone and vibration functions 3. All employees should work together as a team, and escort any panic-struck colleagues to safety 4. Security personnel should call the regional emergency hotline 5. Once the threat is eliminated, based on information received from the local authorities, follow evacuation procedures from emergency personnel

Emergency contacts

In case of emergencies we call for help, information, and services on these emergency hot lines.

EMERGENCY CRISIS HOT LINES (REGIONAL)	
National emergency hotline	
Disaster management services	
Air ambulance	
Red Cross	
Gas leak notification hotline	
Fire department	
Police department	
Hospital	
Medical services (mobile)	
Ambulance services	
UTILITY COMPANIES	
Network provider	
Gas	
Plumbing	
HVAC	
Electricity board	

BCDR Activities

Here is what an emergency scenario at Zoho can look like as the recovery activities unfold. The examples below are some of the recovery activities in case of fire, flood and earthquakes, and of course, will vary depending on the nature of the emergency and its impact on business.

How is Zoho prepared for eventualities?

TIMEFRAME	ACTIVITIES
First 3-4 hours	**External communication:** Our communications team collects information from reliable sources and crafts key messages (before, during, and after the disaster), as well as ensures a consistent message across all channels: website, blog, media, news release, social media, etc. The team maintains a list of potential external audiences to contact as necessary: emergency medical services, fire department, police, local government, suppliers and vendors with their contact numbers. Two official spokespersons, the President/Vice President of Zoho and ManageEngine, with a solid experience in working with both print and broadcast media, will be theprimary contact for all media inquiries. The spokesperson typically runs all press conferences, and gives the most analyst and partner interviews during a crisis. All external communication will include details of the disaster including the date and time of occurrence, a description stating the impact of disaster on business, steps being taken to mitigate the risks, recovery, and business continuity, and estimated time for recovery. **Emergency command centers (ECC):** Our emergency command centers are the coordination hubs for disaster response. The BCDRC and response teams personnel gather critical information, coordinate response and recovery activities, and manage employees as the emergency situation demands from these centers. Emergency command center 1: Estancia IT Park, Chennai, India Emergency command center 2: Tenkasi, India **Alternate locations:** In case of temporary or permanent loss of a disaster-struck facility, the 12 offices spread across different countries act as alternate locations. We move our critical business functions to alternate sites that are equipped to provide similar working environments.

TIMEFRAME	ACTIVITIES
First 3-4 hours	Alternate sites may include (but not limited to): • Zoho's alternate site(s) listed here that are not affected by disaster. The sites closer to the affected site can host the essential resources and also assist in recovering business operations. • Temporary worksites: Temporary worksites are set up in case of emergencies with minimal IT systems, telecommunications, and other equipment. • Telecommuting: Employees work remotely from home or alternate locations of their choice as Zoho runs on cloud applications. **Critical teams and resources:** In the BIA phase of this plan, we identified the critical teams and employees that are considered essential during an emergency or disaster. These critical business units such as customer-facing teams (presales, sales, customer support), and their resources are moved to alternate locations. Minimal resources from other critical business units, such as HR and Facilities report to work regardless of conditions. **Availability:** Application data is stored on resilient storage that is replicated across data centers. Data in the primary data center is replicated in the secondary in near real time. In case of failure of the primary data center, the secondary data center takes over and the operations are carried on smoothly with minimal or no loss of time. Both the centers are equipped with multiple ISPs. We have power back-up, temperature control systems and fire-prevention systems as physical measures to ensure business continuity. These measures help us achieve resilience. The live status and historical status data (30 days) of cloud services can be seen at **status.zoho.com / status.zoho.eu /status.zoho.in / status.zoho.com.au.** **Disaster-ready data backups:** Data backup and recovery is critical for recalling data during natural disasters. At Zoho, we perform full and incremental backups to preserve corporate information. These backups are performed on a regular basis for audit logs and files that are considered critical. The backup media is stored in a secure offsite data center, geographically separate from the original.

TIMEFRAME	ACTIVITIES
5-24 hours	**Succession plan:** In case of casualties, activate the succession plan that lists who replaces the BCDRC, senior managers, managers, team leads during an emergency if they are not available to carry out their responsibilities. **Stabilize the situation:** The disaster situation is stabilized to save lives, and is usually accomplished at the response stage. However, some stabilization activities, such as removing records from the disaster location, and isolating affected systems, are accomplished before damage assessment to prevent further damage to the records and information, as well as to other assets. **Damage assessment:** Once a disaster is declared, the DRT should be mobilized. Damage assessment is accomplished as quickly as conditions permit by the DRT (under the direction of the location authorities) to assess the damage to: • Essential hard copy records (files, manuals, contracts, documentation, etc.) and electronic data. • The site(s), e.g. environmental conditions, physical structure integrity, furniture, and fixtures. Damage assessment helps us gauge the extent of damage: what can be replaced, salvaged, or reconstructed. The results of the damage assessment are documented in the damage assessment and evaluation form. (Check the forms section below for a complete list of forms that we use during emergencies). This helps develop a restoration priority list, identify facilities, vital records, and equipment needed for resumption of activities. The EMT and DRT gather all the information regarding the event and send for BCDRC's review. The decision to move to the business continuity phase is made at this point. If the situation does not warrant this action, then the EMT and DRT continue to address the situation at the affected site(s). **Supply chain:** In times of disaster, our supply chains that were functioning well can experience significant disruption. We have identified a list of key backup vendors for all essential equipment and supplies so we can switch to these vendors in the event the primary vendor is also affected by the disaster.

TIMEFRAME	ACTIVITIES
Days 2-4	**Salvage operations at disaster site:** The salvage operations now begin for damaged IT systems, furniture, workstations, and records with appropriate procedures. The activities include: • Isolating and removing affected systems, furniture, and other equipment from the disaster site. • Sending the systems and equipment for salvage to the respective vendors for repair. • Organizing the undamaged systems equipment • Cleaning all workstations including the furniture, the undamaged IT systems, and other equipment. • Removing debris and making sure the facility is restored to normal. **Move critical resources back to primary site:** As soon as the primary site is stabilized and repaired, the critical resources are moved back into the primary site.
Days 5-14	**Bringing back business as usual:** In the event of total facility destruction, efforts begin for fully rebuilding the facility, while the critical employees continue to work from alternate locations, and other employees work from home. In case of partial damage, the facility is rebuilt in the shortest time possible, and all employees are moved into the primary facility. Once all the IT systems, records, data, supplies are restored and normal operations return for the organization, external communication is sent out to customers, partners, press, and concerned authorities.

Forms

Disaster form:

In the event of a disaster, the on-duty personnel make the initial entries on a disaster form. This form captures a chronological log of the business impact reported during the event. It is then forwarded to the ECC, where it is continually updated. The running log remains active until the disaster ends and its business as usual.

Disaster form

Date and time	Type of event	Location	Building access issues	Projected impact to operations	Running log (ongoing events)

Critical equipment status assessment and evaluation form

Date and time	Type of event	Location	Equipment	Condition	Salvage	Comments

Critical equipment status form:

OK - Undamaged
DBU - Damaged, but usable
DS - Damaged, requires salvage before use
D - Destroyed, requires reconstruction

BCDR Approvals

Once the BCDR plan is completed, including the estimated costs for recovery, it is submitted for a formal approval to the BCDRC. The BCC obtain the support and buy in of the senior management to emphasize the senior management's commitment to the BCDR process and its importance.

Implementation and training

We've now created a BCDR plan, and it's now part of our mainstream processes and policies. The last step is training those who will use the BCDR plan, including those who are not part of its development. The training can include walk-throughs, mock disaster drills, or component testing.

The DRT and EMT teams choose disaster scenarios that can realistically happen. For example, they can build a scenario around a fire accident to conduct mock fire drills. The firedrills are conducted every six months to check the reaction of the employees, the efficiencies of the fire alarm and fire fighting systems, execution of evacuation procedures by the emergency personnel, and the disaster response and recovery activities.

We also train our IT and security teams in disaster response and recovery activities such as phishing attack drills, first level diagnostics such as device maintenance to get them up to speed as they are instrumental in keeping our systems available and accessible in an emergency.

Continual improvement

We've now created a BCDR plan, and it's now part of our mainstream processes and policies. The last step is training those who will use the BCDR plan, including those who are not part of its development. The training can include walk-throughs, mock disaster drills, or component testing.

The DRT and EMT teams choose disaster scenarios that can realistically happen. For example, they can build a scenario around a fire accident to conduct mock fire drills. The firedrills are conducted every six months to check the reaction of the employees, the efficiencies of the fire alarm and fire fighting systems, execution of evacuation procedures by the emergency personnel, and the disaster response and recovery activities.

We also train our IT and security teams in disaster response and recovery activities such as phishing attack drills, first level diagnostics such as device maintenance to get them up to speed as they are instrumental in keeping our systems available and accessible in an emergency.

8000+ employees, spread across 12 offices in several countries serving over 50 million users across the globe.

Yet, Zoho makes a sudden transistion to work-from-home in just 3 days!

How did we make this unimaginable switch?

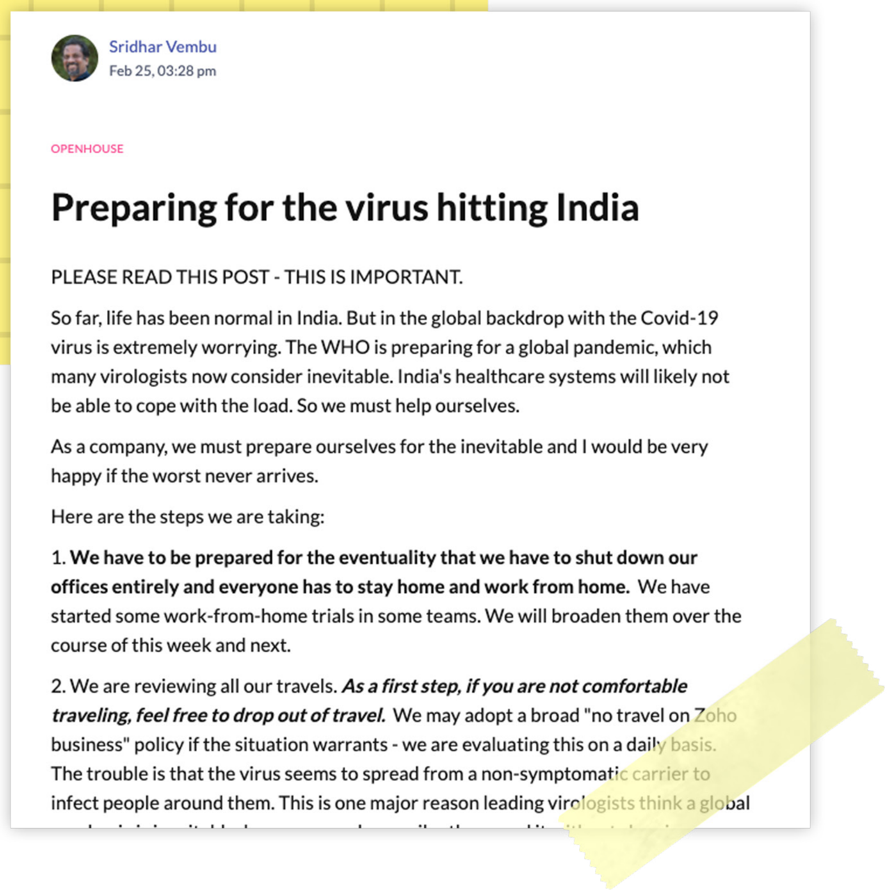
A Covid -19 case study

Chapter 03

Covid-19

A case study

Message from CEO & early warning



Sridhar Vembu
Feb 25, 03:28 pm

OPENHOUSE

Preparing for the virus hitting India

PLEASE READ THIS POST - THIS IS IMPORTANT.

So far, life has been normal in India. But in the global backdrop with the Covid-19 virus is extremely worrying. The WHO is preparing for a global pandemic, which many virologists now consider inevitable. India's healthcare systems will likely not be able to cope with the load. So we must help ourselves.

As a company, we must prepare ourselves for the inevitable and I would be very happy if the worst never arrives.

Here are the steps we are taking:

1. **We have to be prepared for the eventuality that we have to shut down our offices entirely and everyone has to stay home and work from home.** We have started some work-from-home trials in some teams. We will broaden them over the course of this week and next.

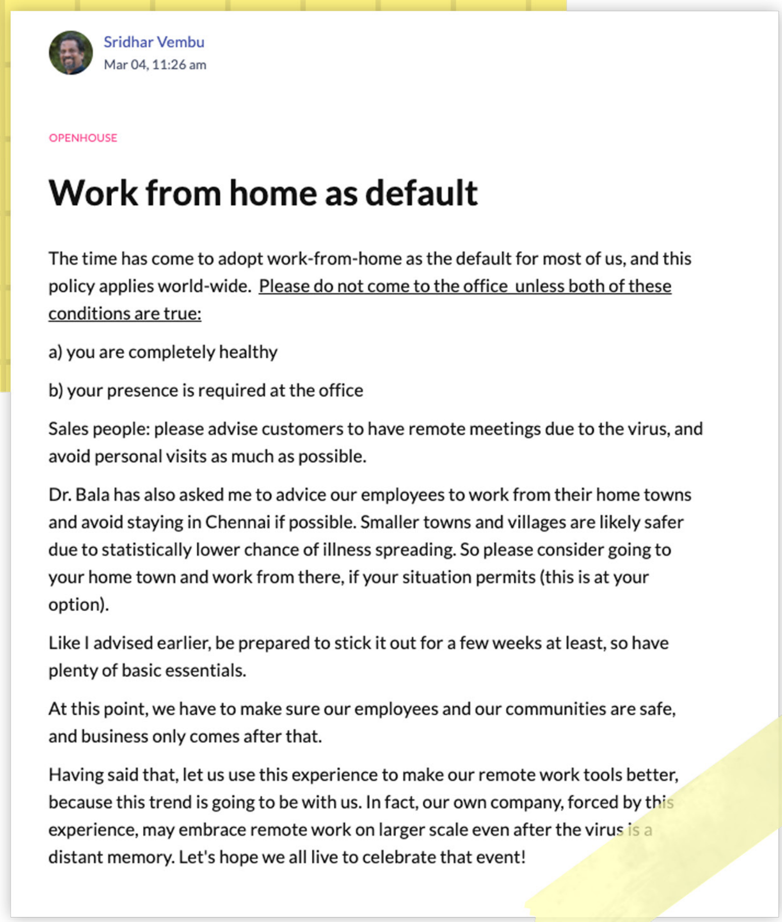
2. We are reviewing all our travels. ***As a first step, if you are not comfortable traveling, feel free to drop out of travel.*** We may adopt a broad "no travel on Zoho business" policy if the situation warrants - we are evaluating this on a daily basis. The trouble is that the virus seems to spread from a non-symptomatic carrier to infect people around them. This is one major reason leading virologists think a global

In February 2020, we faced a global outbreak of COVID-19 that underlined the substantial risk of major global operational disruptions.

25 February, 2020 3:28 PM (IST):

Late February, we received a message from our CEO's desk asking the 10,000+ workforce to brace themselves for the worst, and to deliver their best. He also hinted on the expected economic downturn that would continue through most of 2020, and noted that the biggest challenge would be to sustain a meaningful level of operation through the next six to nine months. The message also listed the timely measures that need to be taken in light of the pandemic and as part of our written BCDR.

The big announcement, after a tough call



Sridhar Vembu
Mar 04, 11:26 am

OPENHOUSE

Work from home as default

The time has come to adopt work-from-home as the default for most of us, and this policy applies world-wide. Please do not come to the office unless both of these conditions are true:

a) you are completely healthy

b) your presence is required at the office

Sales people: please advise customers to have remote meetings due to the virus, and avoid personal visits as much as possible.

Dr. Bala has also asked me to advice our employees to work from their home towns and avoid staying in Chennai if possible. Smaller towns and villages are likely safer due to statistically lower chance of illness spreading. So please consider going to your home town and work from there, if your situation permits (this is at your option).

Like I advised earlier, be prepared to stick it out for a few weeks at least, so have plenty of basic essentials.

At this point, we have to make sure our employees and our communities are safe, and business only comes after that.

Having said that, let us use this experience to make our remote work tools better, because this trend is going to be with us. In fact, our own company, forced by this experience, may embrace remote work on larger scale even after the virus is a distant memory. Let's hope we all live to celebrate that event!

04 March, 2020 11:26 AM (IST):

On March 04, word came from our CEO that it is time for us to embrace the remote-work culture.

Our workforce of more than 8,000 individuals, spread across 12 offices globally, serving over 50 million users across the globe made the jump to remote work culture sound impossible, but it was also a game-changing decision—one we don't regret! Zoho was one of the first technology companies to switch to the work from home model in the face of COVID-19.

Kicking out COVID-19

Zoho is a people-centric company. The health and safety of our employees comes first. As stated earlier, we acted early. Over the last two years, our employees have been travelling a lot for meetings, workshops, seminars, and trade shows. We also have our support and pre-sales teams sitting at customer locations. Our first step was to call all our employees back home to our Estancia office in Chennai, India.

We also put in place several measures including increased precautions at our facilities based on WHO and local government recommendations. We are constantly monitoring the situation, following government directives, and our HR and admin teams are frequently communicating updates to our employees across the world.

Directives we follow:

- The campus is to be operational under the restricted access mode, and only critical resources such as IT system admins and other NOC resources will be allowed inside the campus. These resources can access the campus with written consent from the HR team.
- Common areas such as conference rooms, gyms, and recreational areas are to remain closed.
- All Zoho and ManageEngine events and business trips (both domestic and international) should be canceled (until further notice), and before the government announces flight bans, as possible.
- Employees returning from travel from high-risk countries will be asked to quarantine for 14 calendar days (even when they didn't show any symptoms), and should not come into physical contact with other employees during this time. After the 14-day quarantine period, the employee will be tested by the in-house doctor, and get a note saying the employee is at no risk before being able to return to work on campus.
- Isolation rooms are set up and temperature screenings help safeguard individuals on campus.
- The in-house doctor will monitor the health of the working employees. If the working employees have symptoms, such as cough or fever, they are to work from home.
- Sanitizers and N95 masks will be kept in prominent places inside the Zoho premises.
- All employees will undergo temperature checks using thermal scanners, wear masks at all times, and use sanitizers liberally.

When an employee is tested positive and shows symptoms of illness, we provide continued support and monitor the employee's health condition. We have also enforced the use of contact tracing forms to help track individuals who have come in tract with the affected employee using low-code software that provides a way to create easily distributable online forms and apps. The employee, including the contacts, are required to self-quarantine for a mandatory 14-day period They are to return to Zoho only after a full recovery, and with a doctor's note confirming their recovery. We immediately shut the workplace to sanitize and decontaminate all areas, including the common areas (washrooms, lunch hall, pantry) that the employee may have accessed.

Following this, an external communication is sent out to the local government, health care authorities, stakeholders, partners, and media.

Zoho runs on Zoho

Over the last few months, we have been supporting customers, developing new product capabilities, undertaking product fixes, planning future releases, delivering service packs, and more utilizing our work from home model.We have been accomplishing this as closely as possible to the way our organization operated before the pandemic surfaced.

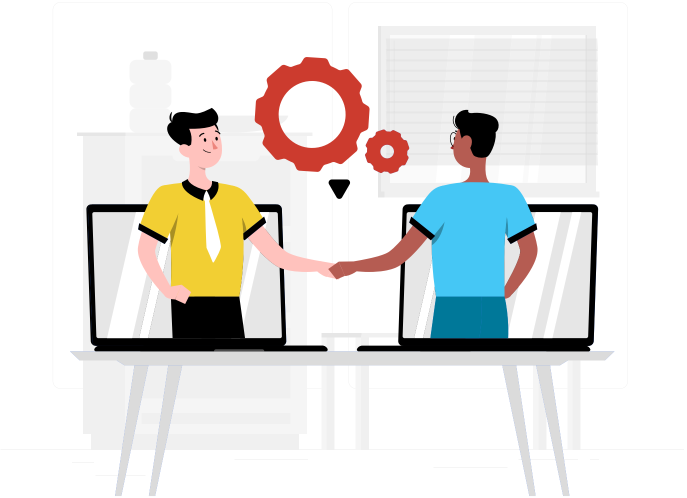
Surprisingly, for a company our size, we don't use third-party business software. We've always run all our operations in the cloud—sales, marketing, customer support, finance, legal, IT etc.—using our very own suite of more than 45 applications. Here's a roundup of some of the most important tools that let us lead the charge on remote culture.

Communication and collaboration:

We come together online to collaborate in real-time using Zoho Connect, Cliq, and Mail,and work as if we were still in the same building. Nearly all of our conversations happen on Connect, so anyone can chime in and catch up on what's happening across other teams and departments. The teams from different time zones can easily gain context and pick up where others left off. The HR and admin team use these applications to relay work from home and COVID 19 announcements, and to keep everyone in the loop.

When communication starts to get a tad confusing, we can quickly hop into video conferencing the same way that we'd walk to a team member's cubicle in our office setting. While nothing comes close to in-person meetings, Zoho Meeting and Showtime help mirror this interaction and let us have meaningful conversations and clear any setbacks.

Whether it's outlining the COVID-19 policies or crafting this e-book, Zoho WorkDrive lets us get our work done. It is a fantastic content collaboration platform that lets us simultaneously write, edit, comment, and share from one open and shared workspace, regardless of the time zones.



Managing projects:

Many of our product teams use Zoho Projects to assign, track progress, and stay on top of our projects especially our product releases. Without Projects, our teams will be running in circles and missing important deadlines. It's also a blessing for our managers as it helps them know people aren't slacking off.

There is more. Our sales and marketing teams use Zoho Campaigns, CRM, and Zoho Social. Our support teams serve customers using Zoho Desk.We hire people with Zoho Recruit, manage them with Zoho People, and balance our books using Zoho Books.

Zorro saves the day (yet again!)

Our IT infrastructure is the backbone of our business operations. Zorro, our network administration team, constantly works behind the scenes long after we leave for the day. When they are not fixing our laptops or recovering lost files, they are firefighting a major incident. The things they do to keep our business running is nearly superhuman. Zorro often handlesa small number of remote workers on an ad-hoc basis. This time around, more than 8,000 in our workforce (including the CEO) went remote overnight. Zorro is hustling every day to:

Secure our data

We use multiple devices (smartphones, laptops, tablets, and desktops) and multiple operating systems (iOS, Android, Windows, and Chrome). Going remote means our devices are outside the wall. As long as our devices are outside and online, our data is at risk.

Today, remote endpoint management and security is Zorro's top priority. They support our employees taking full remote control over the employee-owned and company-owned devices to provide secure updates, manage patches, deploy software, and manage licenses, all the while keeping track of malicious activities across these endpoints.

Virtual private networks (VPNs) are installed to establish a secure connection between our employees network and Zoho's internal network. Once connected, our employees can access the resources on our network just like their devices were physically plugged in at the office using their own unique and confidential username and password.

All of Zoho's cloud applications use a highly reliable single sign-on (SSO) mechanism. While we enjoy the SSO experience, Zorro manages all user accounts, monitors our activities in real-time, and enhances security multifold within the organization. Further, multi-factor authentication (MFA) enables a two-step verification process across all Zoho applications. One extra step while logging into our accounts saves us all from security nightmares forever.

Monitor and respond to incidents

As stated earlier, cyber attackers are not taking time off during the pandemic. While we are distracted trying to contain the virus, Zorro and our NOC teams are more cautious than ever. NOC is monitoring our network, websites, servers, and applications at all times to take necessary action when a critical event such as a network outage happens.

Troubleshoot issues

The cubicle-to-couch shift gave us all time to cook lunch, do laundry between tasks, or walk our pets. Until, reality set in. On a regular work day we might experience an"account locked" message, be unable to take a campaign live, discover our Adobe license expired, face browser issues, or be unable to set up VPN are regular IT requests. But the added complication now is thateveryone is remote.So, our IT PitStop technicians now ask for our permission to take remote access control of our devices to troubleshoot issues and fix all our tech problems.

Manage the influx of IT tickets

We still need equipment from our quarantined work sites (laptops, chargers, mobile phones, mouse, or sometimes even personal items forgotten at our workstations). Our IT PitStop technicians collect the data they need: laptop model, charger type, workstations IDs, etc. using our ITSM tool. With more context, they can respond to tickets easily. They also pass on information such as gate pass number and the point of contact to collect our equipment and belongings using this tool.

Zorro has also made several ITSM-based workflow improvements for business teams—HR, Finance, Legal, and so on to collaborate and work better.

Enable password resets

Let's be honest. Two weeks is all it takes for us to forget our passwords. We still get locked out of our accounts, but our pitstop technicians help us securely self reset our passwords, and unlock our accounts from the comfort of our homes.

Identify and manage vulnerabilities

As cyberattacks spiked after COVID-19, Zorro is constantly looking for new threats. When a vulnerability is identified, Zorro quickly patches the flaws before they lead to a breach, in the processprotectingZoho from falling a victim to cyberattacks.

Manage privileged access

Some of our user accounts have more significance than the others and have super privileges. Their elevated capabilities and access puts these accounts at a higher risk of being compromised. Zorro monitors all privileged accounts, alerting senior management if any suspicious activity is performed from those accounts.

Some of the activities or tasks such as major changes to a server or network configurations also need privileged access.

Manage assets

Since most of our employees moved to their hometowns during the lockdown, they have taken the company owned assets (smartphones, laptops, etc.) allocated to them. Zorro has to maintain a sound asset inventory and manage licenses, so post COVID-19, when our employees are back at office, we can ensure the assets are accounted for.

Share knowledge

With work from home becoming the new normal, some of our distributed employees have become more self-reliant. They are accessing Zorro's internal resourcesto catch up on articles related to VPNs or firewall issues before reaching out to IT PitStop technicians.

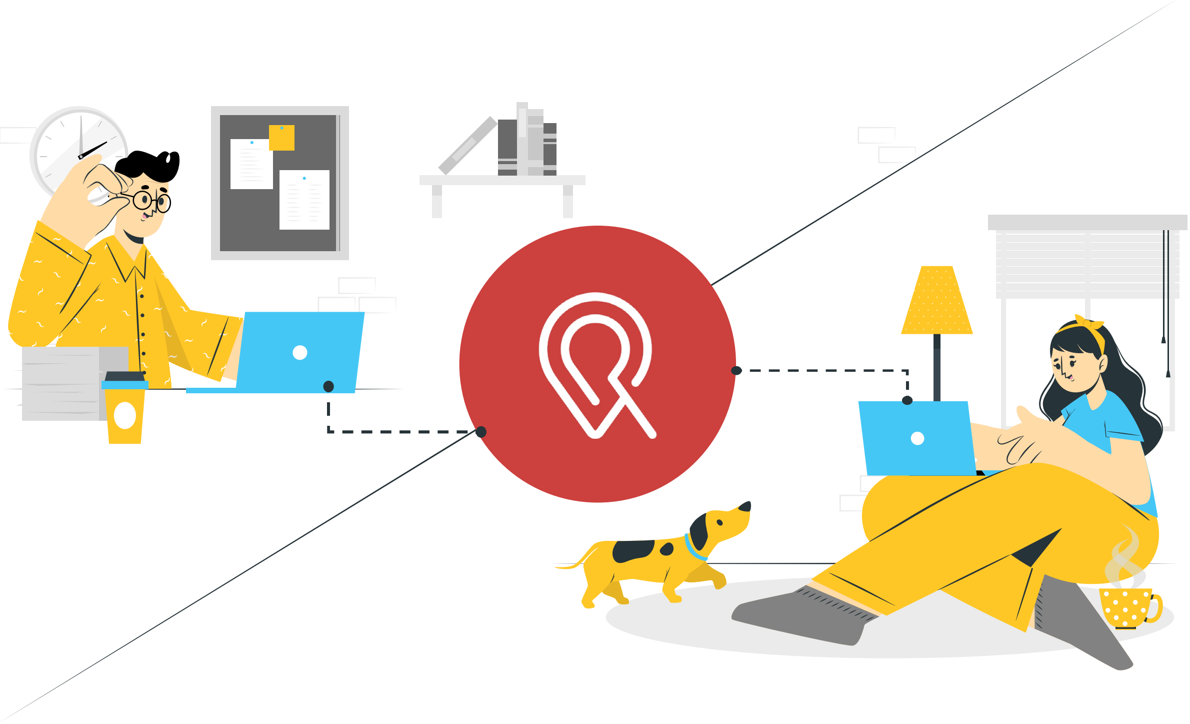
In it together

Our workforce

The switch to WFH has changed our lives. We continue to miss the casual swing bys to the pantry, chats next to the coffee machine, and access to plenty of good food. However, there is also an upside to it: cutting down on long commutes, judgment-free outfit choices, quality time with family and, of course, more productivity.

Yes, that's right. We have seen an uptick in productivity after switching to the work from home model, and we are thankful to all our business teams and employees.

Give back to our customers



To facilitate a smooth work from home transition, IT needs access to critical systems in the infrastructure like servers, applications, databases, and network devices. However, some of our SMB customers have security concerns and are not open for remote access. We feel for them.

We have put together remote working essentials for IT teams to securely and effectively manage their IT infrastructure and enable remote working for their distributed work forces All our ManageEngine tools help customers build multiple layers of security to enable safe remote access to critical IT systems.

On the business side, we have launched Zoho Remotely, a suite of cloud applications that will help with communication, collaboration, work tracking, and remote assistance.

Chapter 04

CONCLUSION

BCDR assessment checklist

If your organization faces an emergency today, do you have the necessary response, recovery, and business continuity processes for dealing with it? We've summed up the pointers that our BCDR efforts are based on.

The below checklist is a starting point for both IT and other organizations to craft a comprehensive BCDR plan. The process will of course differ based on your organizational culture, IT systems and environments, and the nature and severity of the disaster.

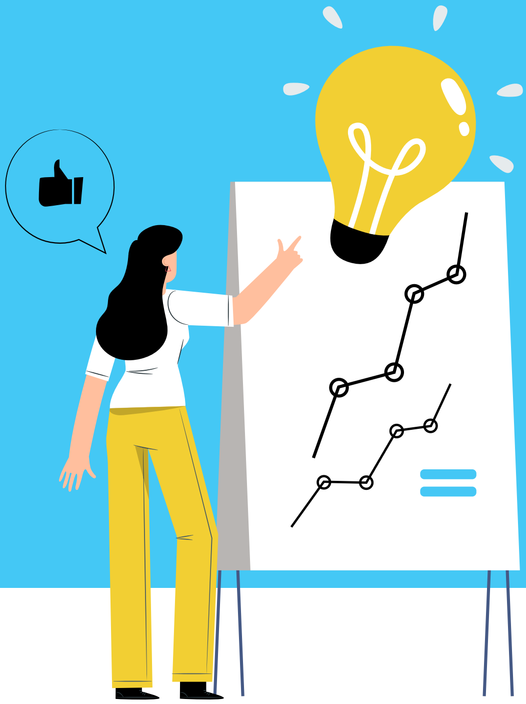
BCDR checklist for enterprises

Purpose and scope	✓ What is the purpose and scope of your BCDR plan? ✓ Does it cover all your critical business units, functions, resources, stakeholders (including customers), and the various kinds of disasters?
Governance and roles	✓ Do you have a senior management team that controls and approves the plan? ✓ Have you identified the team that crafts and modifies the plan? ✓ Have you identified other teams that need to be involved in the BCDR planning, creation, training, and approval processes?
Risk assessment	✓ Have you identified the risks to your organization? Is it a lack of IT security, poor building structure, disasters such as earthquakes, floods and pandemics, man-made accidents such as fire and infrastructure failure such as power failure? ✓ Have you assessed the likelihood of the disasters and evaluated the risks? ✓ Have you identified the measures to control and mitigate these risks? ✓ Have you documented all your risk assessment data?
Business impact analysis	✓ Have you identified the critical business units and their functions? ✓ Have you identified the interdependencies between these business units and functions? ✓ Have you identified the critical resources for the business units and their backups? ✓ Have you identified the critical IT systems? ✓ Have you established the RTO and RPO? ✓ Have you identified the minimum infrastructure, systems, and resources requirements to keep your business running?

BCDR checklist for enterprises	
Business impact analysis	✓ Have you identified the financial impact to your organization? ✓ Have you identified what is at stake for your company should the disaster last for weeks/months such as a pandemic? ✓ Have you documented the impact and created a BIA report?
BCDR planning	**Response** ✓ Have you identified the emergency response teams (including IT) and personnel? ✓ Have you established the notification strategy based on your organizational hierarchy and structure? ✓ Have you identified the assembly points in case of a disaster? ✓ Do you have emergency response procedures for all disaster types? Are all IT arrangements in place such as protecting IT equipment, alternative power backup, and alternative network connection? Is data backed up regularly? Are fire alarm systems in place? ✓ Have you identified the local emergency hot lines? ✓ Do you document every step and do you have forms in place to capture all details, such as in a disaster form? **Communication** ✓ Do you have a communications team to create your communications plan? ✓ Do you have a well-defined internal and external communication strategy in place? **Recovery** ✓ Have you created a timeline of your recovery activities? What will you do in the first 3-4 hours of the disaster, 5-24 hours, 2-4 days, 5-14 days? ✓ Have you identified the emergency command centers and alternate locations for continued business operations?

BCDR checklist for enterprises	
BCDR planning	✓ What are your business continuity measures to ensure availability: data recovery and back procedures, data center resilience, secondary data centers , multiple ISPs, power back-up, temperature control systems, and fire-prevention systems in place? ✓ Does your organization have a succession plan for making key decisions during disasters? ✓ How will you stabilize the disaster situation? ✓ Do you conduct a damage assessment during a disaster to determine damage to critical assets? ✓ What do you do to ensure continuity of supplies? Have you identified backup vendors?
Implementation and training	✓ Do you provide regular training to all emergency personnel? ✓ Do you conduct mock drills for fire, and IT security, such as phishing attacks, etc. with live simulations? ✓ Have you established the time frames and frequency of these mock drills and simulations? ✓ Do you document the results of the training for continual improvement?
Plan review and maintenance	✓ Do you regularly review and update your BCDR plan to ensure that the plan stays current with the latest information and changes in terms of IT systems, resources, infrastructure and policies?

BCDR best practices



We understand how hard it is to think clearly under the intense pressure of a sudden disaster. One of the best ways to respond to an emergency is to keep calm, and not panic. Here are some best practices to consider in your BCDR journey.

- Let's be honest. No matter how many times the plan is tested and improvised, there will be some last revisions/additions during a real emergency. That's where our quick thinking and creativity come into play. At Zoho, we have made some last-minute revisions to our BCDR plan, such as updating the contact of emergency service providers who have moved to a new location, changing evacuation routes, or reassigning employee responsibilities and tasks at last minute. It happens to the best of us, and there is no reason to panic.
- It's good practice to involve and ask for suggestions on improving the plan from the internal audit, accountant, and legal teams. Legal counsel should also be asked to review the BCDR planning efforts to check for any infringement issues.This is a crucial step that can save organizations from legal implications and huge fines.
- During the initial phase of the BIA, a data gathering model that is less time-consuming and more aligned with how you work in your organization is best. Any effort that is not part of your mainstream business activities, such as business continuity, disaster recovery, and compliance, are usually low on priority for your business units and resources. Any steps that you take to reduce the effort to gather the data can pay off.
- It's best to have data centers in different geographical locations, and preferably in areas that less prone to disasters.
- Test the BCDR plan in a realistic way with all resources involved to ensure it actually works, and then make the necessary tweaks.
- Lastly, ensure the plan is accessible to all involved parties even in the event of a disaster.

Final words

In a way, we'd agree that COVID-19 is a wake up call for most organizations. It proved that disaster can strike at any time, and the impact can be felt worldwide.

Assuming, then, that senior management teams are all set on ensuring business continuity and business teams are gearing to create or ramp up an existing plan — we hope this book is of help to all of you and wish you all good luck in your BCDR efforts.

Until next time.