A BEGINNER'S GUIDE TO BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

SCALE COMPUTING

Why do you need a BCDR Plan?

Downtime, data loss, and data corruption, no matter how they happen, can have a serious short-term and long-term impact on a business. Customers can lose faith, as can shareholders, and there's also the possibility of regulatory or government fines. So what should be done if disaster strikes? And equally important, what constitutes a good disaster recovery plan?

Whether the event is malicious in nature, based on a natural event itself, or attributable to human error - the far-reaching effects of an IT disaster are avoidable with regular planning and continual updating. We all take measures to ensure our personal health, our employees' well-being, our vehicles are maintained, and our homes protected - but precautions, procedures, and policies that affect organizations are often not followed with equal regularity. Consider the levels of impact a disaster can have instantaneously and long-term on any business:

- Financial Losses – **Immediate**
- Operational Dysfunction – **Immediate and Intermediate**
- Reputational Loss – **Potentially Long-Lasting Damage**
- Return to Normal – **Possibly Never**

With good planning in place, recovery times can be minimized or even become unnoticed, which reduces lost revenue and time. System backups, system resiliency, replication strategies, and operational procedures are just some of the elements that make dependable companies actually dependable. An essential investment of time and serious thought, disaster recovery plans are a non-negotiable task for businesses - far from an IT luxury - but an absolute need.

Get Planning

Responsibility for business continuity and disaster recovery (BCDR) planning has traditionally rested with the IT department. Unfortunately, this approach has led to the creation of recovery plans that fail to align with the broader needs of the business. It's important to recognize that BCDR planning extends beyond the realm of IT. A collaborative effort across all internal departments and stakeholders is essential to ensure the effectiveness of the plans, as to be successful they need to be far-reaching.

Outlined here is a plan template designed to offer a general outline of steps, aiding in the formulation of your specific plans. It is imperative to conduct thorough research and gain a comprehensive understanding of BCDR principles before initiating the development of a recovery plan.

Before starting, please understand that establishing a BCDR program is a substantial undertaking, and we are here to discuss the IT portion. The aim of your BCDR plan is to guarantee a prompt and smooth response to disasters, all the while reducing potential risks and expenses incurred by information systems and business operations.

These stages, detailed in the subsequent sections, outline a structured framework in five steps:

- **Assess** crucial business data, systems, and applications
- **Develop** expected deliverables
- **Manage and maintain** your plan to ensure it remains current
- **Validate** the effectiveness of your plan through testing
- **Trigger** activation when deemed necessary

Assess

The BCDR planning process begins by evaluating your essential data and systems and identifying vulnerable aspects of your business.

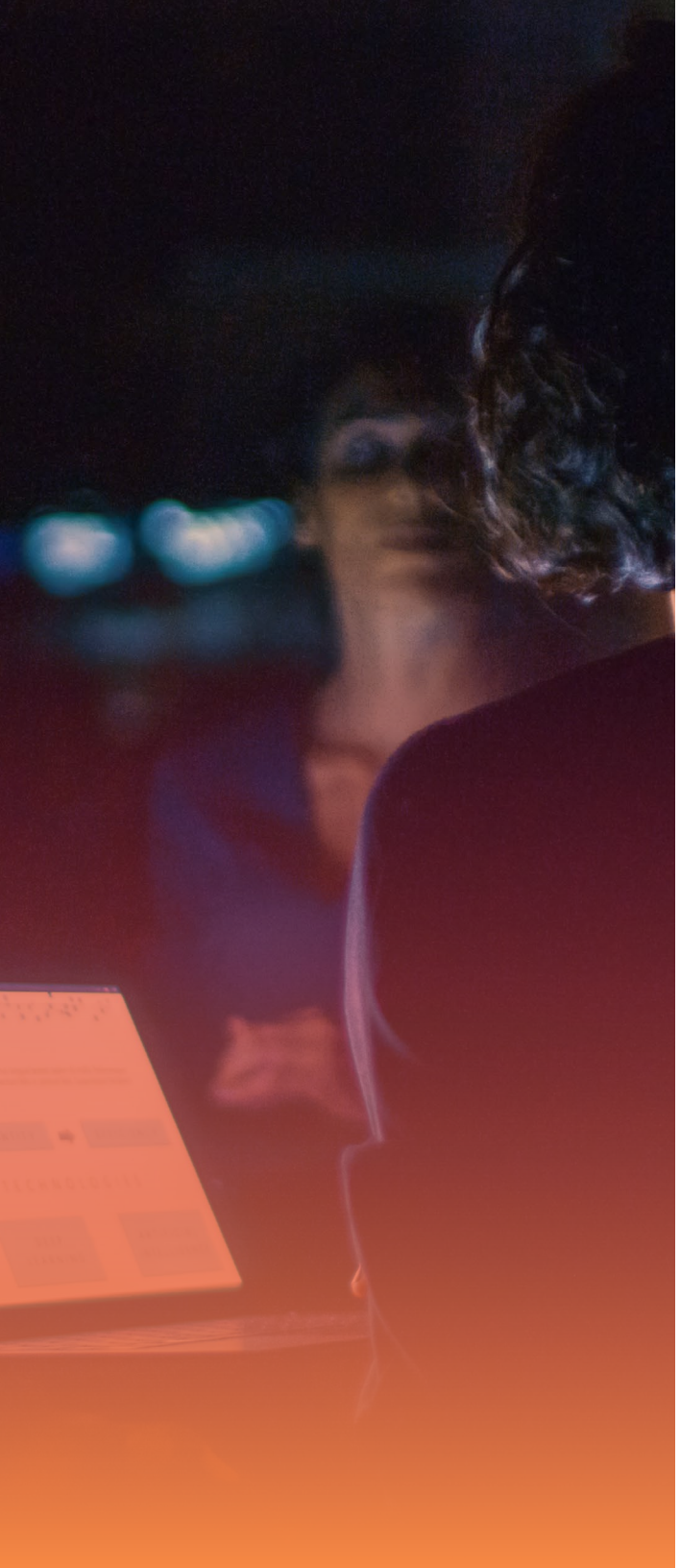
COORDINATE COLLABORATIVE STRATEGIC PLANNING SESSIONS

Host collaborative strategic planning sessions that include a diverse set of teams. Ensure representation from all departments, comprising individuals with varying job titles and responsibilities. Create Disaster Recovery teams and clearly state roles and responsibilities that need to be completed for different types of disaster responses through the use of Emergency Response Procedures.

ESTABLISH OBJECTIVES

Craft goals tailored to the unique characteristics of your business. A few illustrative examples might include:

- Minimizing disruptions to regular operations
- Restricting the disruptions and damages
- Mitigating the economic impact of interruptions
- Creating pre-arranged alternate operational methods
- Training personnel in emergency protocols
- Enabling a seamless and swift service restoration process



UNDERSTAND CRITICAL RESOURCES AND FUNCTIONS

Here, you will create a comprehensive inventory of mission-critical data, locations, and the resources essential for recovery.

- Document profiles for software applications and hardware, encompassing data and voice communications, personal and remote devices, and public networks
- Understand volume constraints
- Identify pivotal records, such as those related to HR, Legal, Finance, and IT.
- Outline interdependencies between servers, systems, and business requisites

TIER APPLICATIONS BY DEGREE OF CRITICALITY

Recognize that not all data, systems, or applications hold equal importance. Document and classify them based on their criticality. Consult with the respective owners from various departments to ascertain their tolerance levels for potential downtime. Common tiers of classification are:

- **Tier 0** - Mission-Critical Systems - Highest level of business function, minimal downtime is tolerated
- **Tier 1** - Business Important Systems - Important to the business, but have some flexibility with downtime
- **Tier 2** - Standard Business Systems - Most common tier for applications
- **Tier 3** - Low Priority Systems - Business utilizes applications, but low reliance on daily operations

DEFINE RTO/RPO

How long can your business function without data and resources, and to what point should they be recovered?

- **Recovery Time Objective (RTO)** – How long can the business or department be without service?
- **Recovery Point Object (RPO)** – To what point should they be recovered? How much data can the business or department afford to lose?

These must be prioritized from both business and technical perspectives.

IDENTIFY VULNERABILITIES AND SCENARIOS

Now that you have conducted a comprehensive analysis of your requirements and timelines, the next step of your assessment is identifying areas of vulnerability within your critical data. Subsequently, you should formulate plans to address a range of potential scenarios. For instance, recovering a single employee's lost email differs significantly from orchestrating a full recovery following a cyberattack.

- Document your existing backup or recovery procedures
- Assess the susceptibility of your systems
- Address various disaster types: natural incidents, inadvertent file deletion, hardware or software malfunctions, cyberattacks, as well as the loss or compromise of remote devices

WEIGH COSTS AGAINST RISKS

Given the multitude of variables inherent in disaster recovery, accurately determining total costs can pose a challenge. Costs serve as a substantial hurdle when establishing effective disaster recovery solutions, and these costs must be weighed against the risk of not achieving a successful recovery.

- Hardware and software expenses – consider the replacement costs of cold storage, applications, and servers
- Non-compliance fines
- Potential reductions in stock value or eCommerce transactions
- Supply chain disruptions
- Indirect costs related to brand perception, reputation, employee morale, and satisfaction
- Odds of events and the likelihood of each occurring

Develop

The development of your BCDR plan's design is rooted in the insights you've gained and documented during the assessment phase. As you craft your DR plan's design, make sure to record resources and anticipated outcomes, prioritize simplicity, and try to automate processes wherever possible.

PRIORITIZE USE CASES BY BUSINESS UNIT

- Tailor groups according to individual departments or workloads
- Prioritize business-critical functions

CREATE TIMELINES FOR ACHIEVING OBJECTIVES

- Network Security
- Cold/Hot Storage
- Physical/Virtual Machines
- Mobile Devices
- Remote User Access, WAN

CREATE AN EMERGENCY RESPONSE PROCEDURE

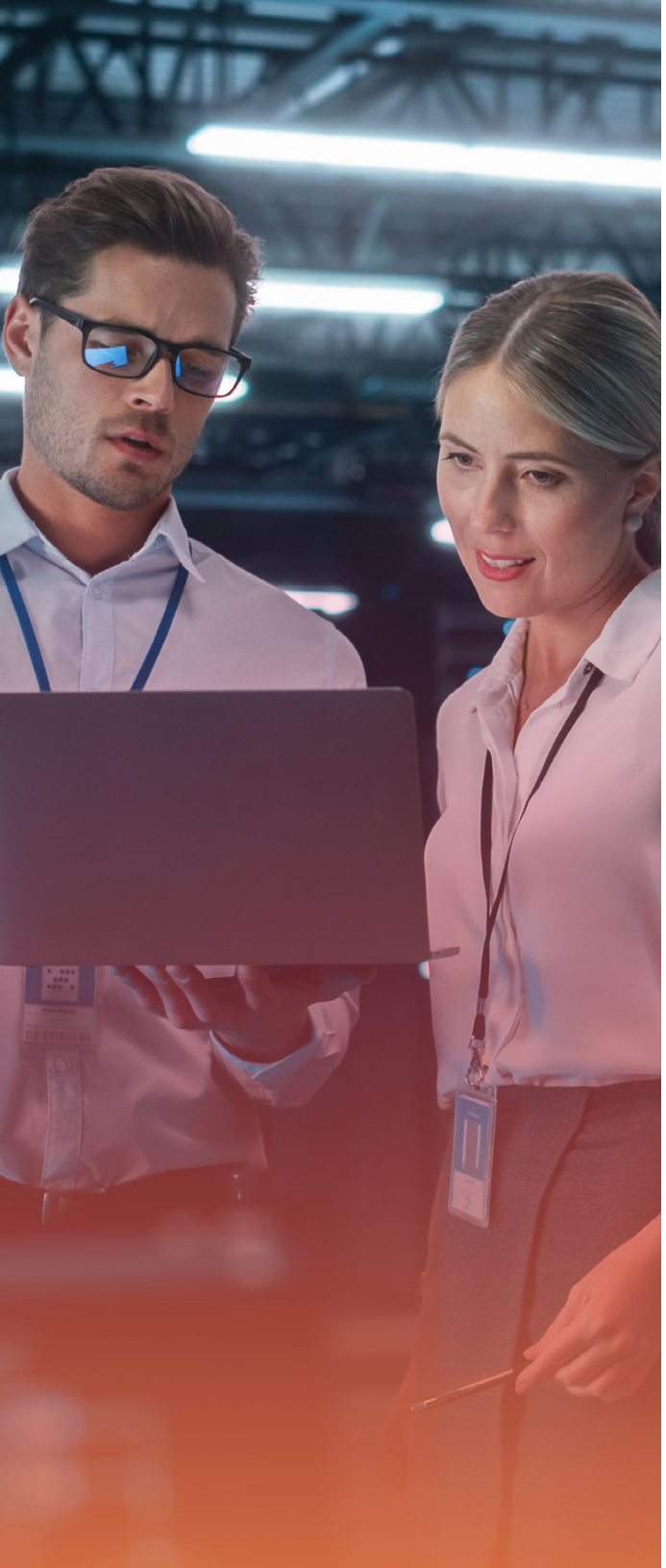
- People to be notified in the event of a disaster (first point of contact, second point of contact, etc.) and clearly state the roles and responsibilities of the point of contacts and action plan
- Plan for deploying the Disaster Recovery Team
- Communication channels and internal/external documentation for notifying stakeholders

ORCHESTRATE AND AUTOMATE

- Runbooks

For your DR plan to seamlessly initiate as needed, your design must encompass the subsequent interconnected strategies and procedures.

DEFINITIONS	EVALUATION	APPROVALS	OPERATIONS	COMMUNICATIONS
Identify specific disaster conditions based on factors such as type, severity, impact, and duration that will trigger the activation of your plan.	Determine whether the established activation criteria have been satisfied in potential disaster scenarios.	Ensure you have the plan activation approvals, involving IT personnel, business leaders, and corporate executives.	Provide facility and system support for all activities linked to plan activation. This includes designating a central site where the majority, if not all, recovery undertakings can be executed.	Inform all stakeholders - employees, customers, vendors, and the public if deemed necessary—about decisions and actions associated with plan activation.



Manage and Maintain

Always keep your disaster recovery plan up to date. This should occur whenever new hardware, software, or systems are integrated, network access is altered, or changes in stakeholders occur. Neglecting these updates can result in your DR plan failing to function when it's most needed!

Validate

Before you ever need to activate your BCDR plan, it's imperative to carry out extensive testing and validation.

Execute your testing in a controlled, non-production environment, encompassing diverse scenarios that account for various types of disasters and pertain to all business segments. Should any aspect fail to function as intended, make the necessary adjustments to your plan.

This phase entails the following key activities:

- Clearly outlining the purpose and approach of the tests
- Identifying teams responsible for conducting the tests
- Structuring tests to encompass a range of outage scenarios
- Executing the tests virtually, through table-top simulations, or on a full-scale basis
- Analyzing the test results
- Adapting the plans based on insights drawn from testing

How your plans are tested will depend on the defined recovery strategies selected to meet your business's recovery prerequisites. Develop testing protocols to ensure the written plans are both precise and all-encompassing.

It cannot be emphasized enough: consistently subject your plan to testing and exercises. Test, test, and test again!

Trigger

Disasters happen, but your plan is ready. In any scenario, swift action becomes imperative as soon as your BCDR plan is set into motion. Time is the enemy in any disaster scenario, leaving little room for reactive decision-making.

Follow your plan. Respond, recover, and then review to improve your response and recovery capabilities.

Post Recovery Plan

What happens after? Once the recovery is completed, the team will need to generate a post-recovery report. The report should include the following so the situation can be understood and any improvements in the plan can be made:

- Summary of the incident
- Analysis of the response
- Any updates or changes that may be needed
- Suggestions for improvement

10 Reasons You Need to Invest in Disaster Recovery

1. Minimize the impact of any disaster
2. Ensure continuous employee productivity
3. Become far more cost-effective
4. Meet compliance and regulatory requests
5. Access instant recovery
6. Reduce downtime of operations
7. Reduce potential financial losses
8. Reduce liability obligations
9. Minimize the risk of negative exposure
10. Facilitate crisis management

COST OF DOWNTIME BY INDUSTRY

IT	AUTOMOTIVE	MANUFACTURING	HEALTHCARE	BROKERAGE	RETAIL
$145- $450K per hour	$3M per hour	$260K per hour	$636K per hour	$6.48M per hour	$1.1M per hour

COST OF A DATA BREACH

In 2023 the average cost of a data breach globally reached an all-time high of $4.45 million. This represents a 2.3% increase from 2022 and a 15.3% rise from 2020.

DOWNTIME AFTER A RANSOMWARE ATTACK

In 2022 the average length of interruption of a business after ransomware attacks in the United States was 24 days. This is an increase from 2020 to 2021 from an average of 15 days to 24 days for the duration of downtime.

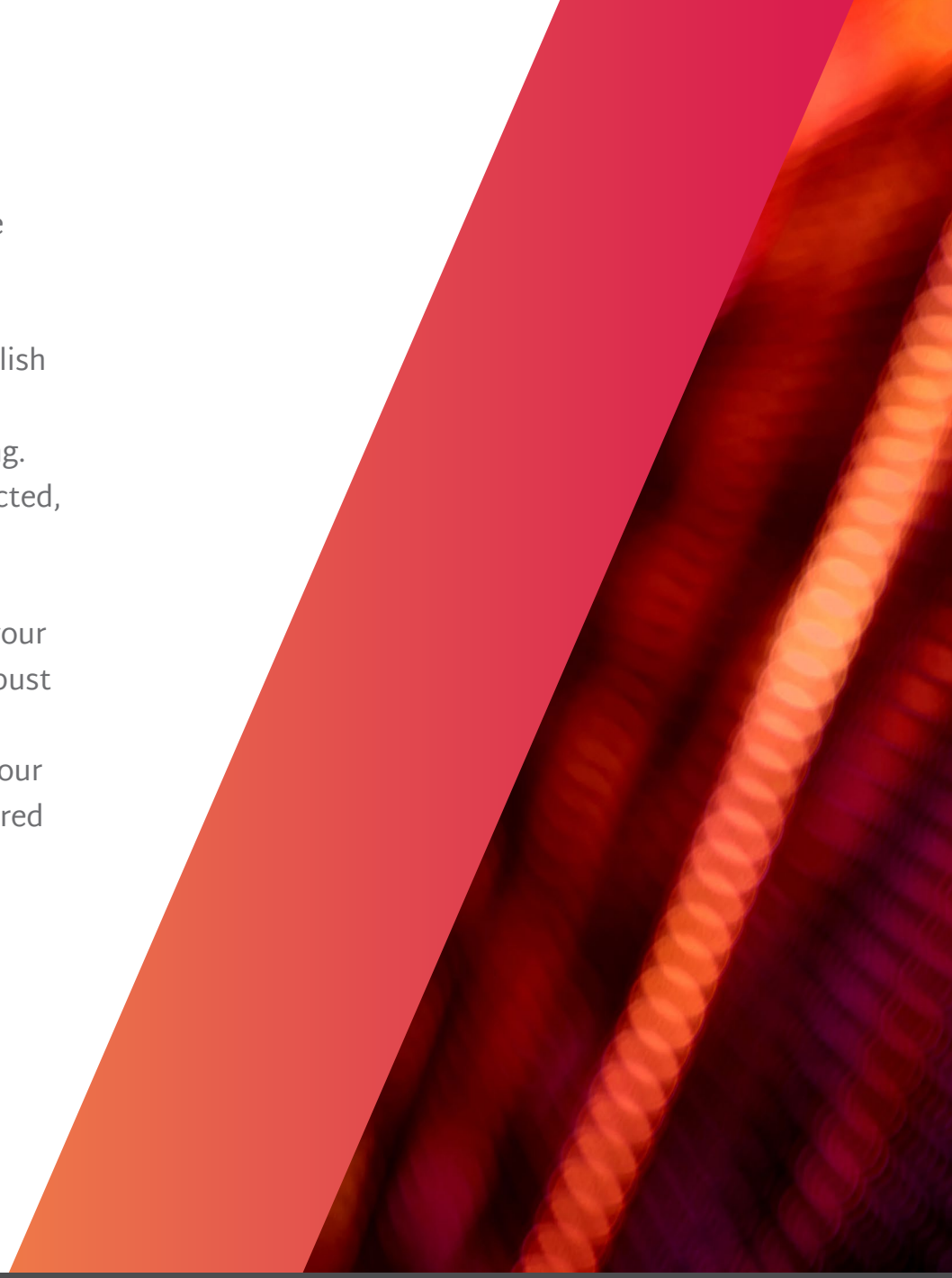
Sources: Gartner, IDC, Atlassian, Statista, Morgan Lewis

Whether it's a mild data loss or a complete business site shutdown, having a well-defined business continuity strategy is crucial. Our Business Continuity/Disaster Recovery Planning Service is designed to help you establish a comprehensive and regulated plan for responding to unforeseen downtime and keeping your business running. Our service ensures that your critical systems are protected, validated, tested, and ready for recovery at any time.

With our expert guidance, you can proactively classify your systems based on their importance and implement a robust action plan for recovery. From planning to deployment, documentation creation, and disaster recovery testing, our service covers every aspect to keep your business prepared and resilient.

For more information on how we can help with your business continuity and disaster recovery, contact us today.

CONTACT US



SCALE COMPUTING

CORPORATE HEADQUARTERS
525 S. Meridian Street - 3E // Indianapolis, IN 46225
P. +1 317-856-9959 // **scalecomputing.com**