ICR – INTEGRATED CONTINUOUS RESILIENCE STANDARD

ICR

Integrated Continuous Resiliency (ICR) Standard - A Guide for Business, IT, and Cloud Resiliency Management

BRCCI
Business Resilience Certification Consortium International (brcci.org)

Copyright © [2023] BRCCI. All rights reserved
Document Reference Number: ICR-2024-v2.2
Document Details: brcci.org/standard

Integrated Continuous Resiliency (ICR) Standard - A Guide for Business, IT, and Cloud Resiliency Management

CONTENTS

ABSTRACT 3

SECTION 1.0 - INTRODUCTION 4

SECTION 2.0 - SCOPE 4

SECTION 3.0 - ICR DESIGN APPROACH 5
Section 3.1 - Program Definition 5
Section 3.2 - Program Architecture 6
Section 3.3 - Business-Technology Interface 6

SECTION 4.0 – RESILIENCY DEFINITION 6

SECTION 5.0 – RESILIENCY PROGRAM ARCHITECTURE 7
Section 5.1 – Segment A: Resiliency Planning Process 8
Section 5.2 – Segment B: Resiliency Program Management 8

SECTION 6.0 – RESILIENCY PLANNING PROCESS 9
Section 6.1. – S1: Resiliency Process Definition 9
Section 6.2 – S2: Resiliency Risk Management 10
Section 6.3 – S3: Business Impact Analysis (BIA) 11
Section 6.4 – S4: Constraints and Dependencies Management 11
Section 6.4.1 - General BCR Constraints and Dependencies 12
Section 6.4.2 - Recovery Requirement Constraints and Dependencies 12
Section 6.4.3 - Availability Constraints and Dependencies 12
Section 6.4.4 - BCR Strategy Constraints and Dependencies 13
Section 6.4.5 - Technological Constraints and Dependencies 13
Section 6.5 – S5: Resiliency Strategy Development 13
Section 6.5.1 - Level A: Critical Business Operations 14
Section 6.5.2 - Level B: IT Services 15
Section 6.5.3 - Level C: Cloud Environment 15

SECTION 6.6 – S6: SKILLS-STRATEGY GAP ASSESSMENT (SGA) 17

SECTION 6.7 – S7: PLAN DESIGN AND DEVELOPMENT 18

SECTION 6.8 – S8: MONITORING AND TESTING 19

SECTION 7.0 – CORE COMPONENT: RESILIENCY PROGRAM MANAGEMENT 20
Section 7.1 - F1: Resiliency objective Management 20
Section 7.1.1 - Understanding the Context 21

 Copyright © [2023] BRCCI (brcci.org)

Section 7.1.2 - Assessing Resiliency Scope 21
Section 7.1.3 - Establishing Resiliency Objectives 22
Section 7.2 - F2: Personnel and Resource Management 23
Section 7.3 - F3: Incident Resiliency Management 23
Section 7.4 – F4: Resiliency Plan Maintenance 24
Section 7.5 – F5: Program Documentation Management 25
Section 7.6 – F6: Plans Integration and Rollout 25
Section 7.7 – F7: Program communication and coordination 27
Section 7.8 – F8: Continual Program Improvement 27
Section 7.8.1 – Program Maturity Improvement 27
Section 7.8.2 – Resiliency Culture Development 28
Section 7.8.3 – Program Quality Assurance 29

SECTION 8.0 – AUDIENCE 30

SECTION 9.0 – TERMS AND DEFINITIONS 31

SECTION 10.0 – COPYRIGHT NOTICE AND PERMISSIONS 38

 Copyright © [2023] BRCCI (brcci.org)

ABSTRACT

Resiliency is not just a trait but has become a critical requirement for organizations in today's challenging business and technology-driven environment. The Integrated Continuous Resiliency (ICR) standard, developed by BRCCI, offers organizations guidance in developing resilience management programs. Emphasizing integrated resiliency and continuous resiliency, the standard advocates the permeation of resilience across all operations and service levels of an organization – from core business functions to IT systems and cloud services.

The scope of the ICR framework extends beyond the traditional business continuity and IT DR practices to address the requirements for integrated and continuous resiliency. Integrated resilience underscores the interconnected nature of an organization's operations and service levels. Meanwhile, Continuous Resiliency introduces a proactive approach to resilience, acknowledging the need to maintain operational stability and service reliability at all times, irrespective of disaster scenarios.

To incorporate “Continuous Resiliency”, ICR expands the definitions of traditional business continuity and IT DR recovery objectives. The resiliency objectives for "Continuous Resiliency" span across both normal operational conditions and post-disaster conditions.

At its core, the ICR standard offers a pragmatic and comprehensive approach to continuity and resilience, extending beyond traditional business continuity and IT disaster recovery practices. The ICR standard guides organizations in developing Business Continuity and Resiliency (BCR) programs to achieve resiliency at all levels, including core business functions, IT systems, and cloud services, and under all operating conditions.

 Copyright © [2023] BRCCI (brcci.org)

SECTION 1.0 - INTRODUCTION

The Integrated Continuous Resiliency (ICR) standard, developed by BRCCI (brcci.org), is a comprehensive framework for continuity and resiliency best practices. This standard offers organizations a unified framework to achieve continuity and resiliency across business functions, IT services, and Cloud environment.

Resiliency is not just a trait but has become a critical requirement for organizations in today's challenging business and technology-driven environment. To navigate these challenges, organizations require a robust resiliency approach that incorporates resiliency across all service levels, irrespective of operating conditions and scenarios. The scope of the ICR framework extends beyond the traditional business continuity and IT DR practices to achieve integrated and continuous resiliency requirements.

- **Integrated Resiliency**: This requirement emphasizes the importance of permeating resiliency across all levels of an organization - from its core business functions to its IT systems and cloud services. A lack of resiliency at one level can compromise resiliency at other levels. ICR offers a holistic approach to implementing an effective resiliency program by integrating resilience at every level.
- **Continuous Resiliency**: ICR introduces the "Continuous Resiliency" concept to underscore the organization's requirements to maintain operational stability and service reliability at all times, irrespective of disaster scenarios. Unlike traditional business continuity frameworks, which often focus solely on preparing for disaster scenarios, ICR recognizes the importance of maintaining resilience even during normal, non-disaster conditions. This proactive approach ensures that organizations are prepared to weather any storm, whether a minor disruption or a full-scale crisis.

The ICR standard guides organizations in developing Business Continuity and Resiliency (BCR) programs to achieve resiliency at all levels, including core business functions, IT systems, and cloud services, and under all operating conditions.

SECTION 2.0 - SCOPE

The ICR standard applies to organizations of all types and sizes and specifies a framework of structure and requirements for assessing, designing, implementing, maintaining, and improving business continuity and resiliency programs. It caters to entities seeking to establish a culture of integrated continuous resilience across all levels, from core business functions to IT systems and cloud services.

As a generic framework, ICR offers various uses and applications. Key applications of the ICR standard include, but are not limited to:

- **Comprehensive BCR Program Development**: Organizations can leverage the ICR standard to establish robust business continuity and resiliency (BCR) programs tailored to

 Copyright © [2023] BRCCI (brcci.org)

their specific resiliency objectives. By following the guidelines outlined in the standard, entities can create integrated frameworks to achieve continuous operational resiliency.

- **Enhancement of Existing BC Programs**: For organizations with existing business continuity (BC) programs, the ICR standard includes requirements to further strengthen and evolve these initiatives into resiliency programs. By integrating the principles and practices specified in the ICR standard, entities can elevate disaster event-focused business continuity capabilities to achieve continuous resiliency under all operating conditions.
- **Integration of BC, IT DR, and Cloud Recovery Plans**: The ICR standard provides a cohesive resiliency framework for organizations with existing BC plans, IT disaster recovery (DR) plans, and cloud recovery strategies. By aligning these disparate plans within the overall ICR framework, organizations can achieve a unified approach to resilience management, with seamless coordination and response across all operational domains.
- **Evaluation and Auditing of BCR Plans**: Organizations can use the ICR standard as a benchmark for evaluating the compliance and effectiveness of their existing BCR plans and programs. Through assessments and audits based on the criteria outlined in the standard, entities can identify both areas of strength and areas for improvement.

SECTION 3.0 - ICR DESIGN APPROACH

The ICR Standard captures the fundamental essence of established standards and guidelines while seamlessly integrating practical, easy-to-follow directives for real-world BCR program implementation. The ICR Framework comprises a BCR lifecycle with seven stages and a singular core component featuring 8 elements to manage these stages. This framework separates the BCR program process from the Program management function while preserving essential interdependencies.

The ICR integrates resiliency at three key levels of the business resiliency program: Program Definition, Program Architecture, and Business-Technology Interface.

Section 3.1 - Program Definition

The traditional BC and IT DR programs are guided by the objective of maintaining operational continuity, and their scope is limited to disaster events. While this definition of objective and scope is adequate for operational continuity, it falls short of achieving comprehensive resiliency.

ICR standard incorporates resiliency within its program definition by expanding the objective and scope of traditional BC and IT DR programs. The resiliency objective is expressed as integrated operational stability of business, IT, and Cloud environments. The operational continuity objective becomes a part of the integrated operational stability objective. The resiliency scope extends beyond the disaster condition to include normal operating conditions. This extension of the

 Copyright © [2023] BRCCI (brcci.org)

scope implies that maintaining integrated operational stability under all operating conditions becomes an integral part of the resiliency objective.

Section 3.2 - Program Architecture

While traditional BC and IT DR frameworks often amalgamate program management components and planning processes, a resilient architecture demands a functional separation between these elements. This separation allows for the delineation of resiliency objectives across three levels:

1. Overall program resiliency objectives
2. Planning process resiliency objectives
3. Program management resiliency objectives.

Section 3.3 - Business-Technology Interface

ICR embeds resiliency within the Business-Technology interface. It views the program planning process as the nexus between business and technology resilience. Unlike conventional BC and DR frameworks where Business Impact Assessment (BIA) serves as the primary interface, ICR extends this interface to encompass additional stages. These additional stages include "Constraints and Dependencies," "Skills-Strategy Gap Assessment," and "Monitoring and Testing."

SECTION 4.0 – RESILIENCY DEFINITION

The resiliency objective definition is based on the "Continuous Resiliency" concept, which expands the definitions of traditional business continuity and IT DR recovery objectives.
The objective definitions in the traditional approach are based on MTDs and RTOs related to the time of a disaster event. Before a disaster event, during normal conditions, the IT organization is concerned with availability objectives such as MTBF (Mean Time Between Failure), MTTR (Mean Time To Recovery), and MTTD (Mean Time to Detection).

However, resiliency objectives for "Continuous Resiliency" span across both normal operational conditions and post-disaster conditions. ICR abstracts both availability objectives and continuity objectives to a higher level. At this higher level, the resiliency objective is expressed as Acceptable Stability Levels (ASL).

The resiliency definition is stated as follows:

> **"Resiliency is a process to ensure Acceptable Stability Levels (ASL) during both normal and disaster periods."**

 Copyright © [2023] BRCCI (brcci.org)

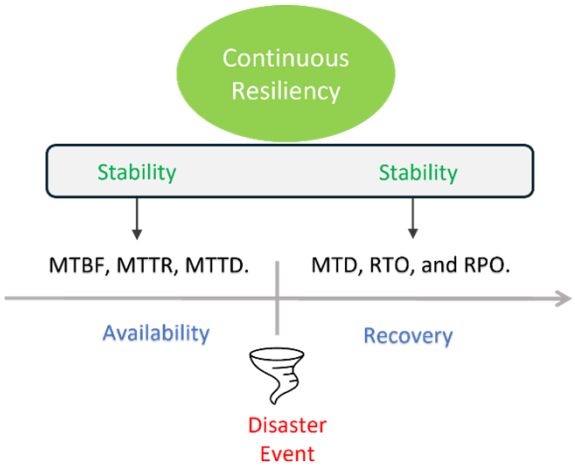

Figure 1 – Continuous Resiliency

SECTION 5.0 – RESILIENCY PROGRAM ARCHITECTURE

Management of the Business continuity and resiliency program involves two distinct but related functions. The first is a resiliency planning process or lifecycle that generally follows a path from plan assessments to design, development, testing, and maintenance. The second is resiliency program management, which is concerned with managing the resiliency planning process. The traditional BC and IT DR frameworks do not separate these two functions from each other.

Separating the resiliency planning process from resiliency program management helps achieve the overall program resiliency objectives. The program resiliency objectives can be divided into more granular levels, with separate resiliency objectives for each function.

Figure 2 - ICR Architecture

 Copyright © [2023] BRCCI (brcci.org)

As shown in Figure 2, the ICR architecture consists of two segments: Segment A and Segment B. Segment A is the resiliency planning process, which consists of 8 stages. Segment B is the resiliency program management, which deals with the program management aspects. The core component consists of 11 elements.

This framework ensures a functional separation of the BCR program process from Program management aspects while preserving essential interdependencies between the two.

Section 5.1 – Segment A: Resiliency Planning Process

Segment A consists of 8 stages, S1 through S8:

- S1 – Resiliency Process Definition
- S2 – Resiliency Risk Management
- S3 - Business Impact Analysis (BIA)
- S4 - Constraints and Dependencies Management
- S5 - Resiliency Strategy Development
- S6 – Skills-strategy Gap Assessment
- S7 – Plan Design and Development
- S8 – Monitoring and Testing

Section 6 describes each of the 8 stages of the Resiliency Planning Process.

Section 5.2 – Segment B: Resiliency Program Management

Segment B, also referred to as the "core component," deals with the program management aspects. The core component is made up of 8 management functions:

- F1 – Resiliency Objective Management
- F2 - Personnel and Resource Management
- F3 – Incident Resiliency Management
- F4 - Resiliency Plans Maintenance
- F5 – Program Documentation Management
- F6 – Plans Integration and Rollout
- F7 – Program Communication and Coordination
- F8 - Continual Program Improvement

 Copyright © [2023] BRCCI (brcci.org)

Section 7 describes each of the 8 management functions.

SECTION 6.0 – RESILIENCY PLANNING PROCESS

Resiliency Plans are developed through a planning process that contains a sequence of key stages or activities. Segment A of the ICR architecture defines the resiliency planning process. Figure 3 represents the planning process as a lifecycle of eight key stages.

Figure 3 - Segment B - Resiliency Planning Process

The remainder of this section describes each of the eight stages of the resiliency planning process.

Section 6.1. – S1: Resiliency Process Definition

This initial stage defines the objectives, scope, constraints, and interdependencies for each of the following seven stages in the BCR lifecycle:

- S.2 - Risk Management
- S.3 - Business Impact Analysis (BIA)
- S.4 - Management of Business Continuity and Resiliency Constraints and Dependencies (e.g., supply chain dependencies, resources)
- S.5 - Development of Continuity and Resiliency Strategies

 Copyright © [2023] BRCCI (brcci.org)

- S.6 – Skills and Capability Alignment
- S.7 - Design and Development of BCR Plans
- S.8 - Testing and Validation of BCR Plans

The objectives, scope, and constraints are aligned with the resiliency objective and definition:

"Resiliency is a process to ensure Acceptable Stability Levels (ASL) during both normal and disaster periods."

Section 6.2 – S2: Resiliency Risk Management

The second stage focuses on assessing and managing risk to Acceptable Stability Levels (ASL). The assessment includes the identification of metrics to measure stability during normal and disaster periods for three core levels: business operations, IT services, and Cloud environment. Examples of metrics for ASL are listed below:

Level A - Critical Business Operations:

For critical business operations, an ASL could be defined in terms of:

- Maximum allowable downtime in hours or minutes.
- Percentage of functionality or service availability.
- Impact thresholds are based on financial loss or customer impact.
- Recovery time objectives (RTOs) for key processes or systems.
- Mean time between failures (MTBF) for essential equipment or infrastructure.

Level B - IT Services:

For IT services, ASL could be defined by:

- Service uptime targets, such as 99.99% availability.
- Response time objectives for service requests or incident resolution.
- Recovery point objectives (RPOs) for data backup and recovery.
- Capacity thresholds to ensure adequate performance under load.
- Mean time to detect (MTTD) and mean time to recover (MTTR) for incidents.

Level C - Cloud Environment:

In the context of cloud environments, ASL may include:

 Copyright © [2023] BRCCI (brcci.org)

- Availability guarantees provided by the cloud service provider (e.g., SLA commitments).
- Data durability and integrity assurances.
- Network latency and bandwidth thresholds.
- Security and compliance requirements, including data privacy and regulatory standards.
- Disaster recovery capabilities and recovery timeframes for cloud-based resources.

A risk management process includes a comprehensive risk assessment, analyzing potential threats to ASL, estimating their likelihood and potential impact, and formulating appropriate mitigation strategies to address the identified risks.

The results and findings from the risk management process form a basis for crafting robust BCR plans. A central objective of a BCR plan is to manage the threats and risks identified during the risk management process.

Section 6.3 – S3: Business Impact Analysis (BIA)

Through the BIA, organizations gain a comprehensive understanding of the critical areas of their business and the potential impacts of disruptions on those critical areas. The BIA process includes the following objectives:

1. Identifying critical and non-critical business functions
2. Assessing the potential impact on critical functions in case of their disruptions
3. Identifying requirements to recover the critical functions when a disruption occurs.

The BIA serves as the foundation for subsequent stages of the BCR lifecycle, as it helps prioritize recovery efforts and resource allocation.

The Maximum Tolerable Downtimes (MTDs) and Recovery Time Objectives (RTOs) are identified as metrics for recovery requirements. The ASL (Acceptable Stability Levels) for the disaster recovery period is defined in terms of the metrics for recovery requirements.

Section 6.4 – S4: Constraints and Dependencies Management

Stage Four of the ICR standard addresses the need for effective management of constraints and dependencies to achieve organizational continuity and resilience. This stage focuses on factors such as supply chain dependencies, resource limits, and regulatory obligations. The overarching goal is to ensure that organizations maintain Acceptable Stability Levels (ASL) across all operational phases. Achieving ASL requires a comprehensive understanding and management of various constraints and dependencies that could potentially impact organizational resilience.

This includes considerations around budget constraints, recovery requirements, availability of critical resources, technological limitations, and strategic challenges. By proactively managing

 Copyright © [2023] BRCCI (brcci.org)

these factors and aligning them with organizational priorities, the ICR standard aims to strengthen resilience and ensure that organizations can maintain ASL even in the face of disruptions and challenges. The ICR standard defines five categories of constraints and dependencies:

1. General BCR Constraints and Dependencies
2. Recovery Requirement Constraints and Dependencies
3. Availability Constraints and Dependencies
4. BCR Strategy Constraints and Dependencies
5. Technological Constraints and Dependencies

These categories are explained in the sections below.

Section 6.4.1 - General BCR Constraints and Dependencies

This category covers a wide range of general factors that could affect the organization's ability to maintain continuity and resilience. Budget constraints are a key concern, as limited finances may hinder robust business continuity measures. Regulatory compliance is also critical, as non-compliance can lead to financial penalties, reputation damage, and legal liabilities. Reliance on external suppliers or partners in the supply chain can introduce risks like disruptions and logistical challenges. Moreover, internal constraints such as staffing limits, communication barriers, and cultural differences may impact the effectiveness of business continuity efforts.

Section 6.4.2 - Recovery Requirement Constraints and Dependencies

The constraints and dependencies in this category are related to factors that influence the ability to recover critical business operations and services in the event of a disruption. Constraints on maximum tolerable downtime (MTD) and recovery time objectives (RTOs) are crucial, as prolonged downtime can lead to significant financial, operational, and reputational damage. Dependencies on specialized recovery teams and expertise are also critical, as skilled personnel are essential for executing recovery plans effectively. Additionally, reliance on external resources like equipment, facilities, and transportation services may impact the organization's ability to resume operations within the necessary timeframe.

Section 6.4.3 - Availability Constraints and Dependencies

This category considers constraints related to the stability of critical resource availability during normal operations. Mean time between failures (MTBF) provides a metric to measure the stability of critical resource availability. Software applications and servers that support critical business operations are considered critical resources. Availability constraints and dependencies also extend to other critical resources like power, telecommunications, and internet connectivity, which are vital for resiliency during normal operations and disaster recovery periods. Dependencies on external service providers, including cloud service providers and

 Copyright © [2023] BRCCI (brcci.org)

managed service providers, may pose risks concerning service availability, data security, and regulatory compliance.

Section 6.4.4 - BCR Strategy Constraints and Dependencies

Constraints and dependencies in this category are related to the limitations faced when developing and implementing business continuity and resilience strategies. These limitations may include constraints on organizational resources, expertise, and capabilities, as well as competing priorities and conflicting goals. Finding a balance between the need for resilience and other organizational objectives, such as cost reduction, innovation, and expansion, can be challenging. Moreover, factors like organizational culture, leadership support, and stakeholder involvement can affect the efficacy of resilience strategies.

Effectively managing these constraints involves aligning business continuity efforts with organizational priorities, engaging stakeholders, and making efficient use of available resources. Proactively addressing these constraints strengthens resilience and ensures uninterrupted critical operations and services.

Section 6.4.5 - Technological Constraints and Dependencies

In this category, constraints, and dependencies are specifically related to critical IT infrastructure and cloud services. This includes limitations in technology capabilities and its management and reliance and dependency on third-party vendors or service providers. These constraints involve hardware limitations, software compatibility issues, network vulnerabilities, or data storage or processing limits. Dependencies on external technology partners or cloud service providers can introduce risks related to service availability, data security, and compliance with regulatory requirements.

Section 6.5 – S5: Resiliency Strategy Development

The preceding stages define the requirements for the BCR program. This fifth stage provides strategies and solutions to satisfy the BCR program requirements such that Acceptable Stability Levels (ASL) are maintained.

The fifth stage includes an assessment of alternative operating models, backup systems and services, and recovery solutions. The assessment considers the critical functions and services, their recovery time constraints, costs, complexity, and feasibility. The strategies and solutions should consider the following operational phases:

Normal Phase: In this phase, strategies are aimed to maintain the continuous stability of operations and services during the normal operational phase. Considerations for strategies include achieving acceptable availability objectives for critical resources and services, minimizing possibilities of disruptive incidents, and effective coordination with vendors and cloud service providers.

 Copyright © [2023] BRCCI (brcci.org)

Prevention Phase: Before a potential disaster, solutions and strategies are needed to prevent or minimize the likelihood of a disruption.

Response Phase: During a disaster, immediate actions are required to stabilize and minimize the effect of a disruption.

Recovery Phase: After an immediate response to stabilize the disruption, strategies are needed to restore the business environment and its operation to normal or to a new environment.

For each of the four phases, the goal of strategies and solutions is to address the ASL risks at three core levels (Levels A, B, and C) as mentioned in S2 – Resiliency Risk Management stage:

Section 6.5.1 - Level A: Critical Business Operations

At this level, the resiliency strategy should safeguard the critical business functions and operations that drive the organization's core functions and value delivery. These critical functions and operations are vital to maintaining revenue streams, customer satisfaction, and overall organizational reputation. The following activities support the development of effective resiliency strategies:

- **Preventive Measures:** The emphasis here is on proactively establishing safeguards. By implementing redundant systems and failover mechanisms, the organization aims to achieve and maintain ASL targets. This ensures that even if one system fails, another is ready to take over seamlessly, minimizing downtime and service disruptions.
- **Business Impact Analysis (BIA):** Understanding the criticality of each business process is essential. Through BIA, organizations assess the potential impact of disruptions on these processes. This analysis helps in determining the ASL requirements for each critical business function, allowing for more focused resource allocation and planning.
- **Resource Allocation:** Proper allocation of resources is key to supporting critical operations effectively. By aligning resources with ASL objectives, organizations ensure that these operations have the necessary support, whether it's in terms of infrastructure, manpower, or financial backing, to meet defined availability and recovery time objectives.
- **Incident Management Planning:** Having a robust incident management plan in place is crucial. These plans outline the steps to be taken in the event of disruptions, ensuring a structured and coordinated response. By adhering to ASL targets within these plans, organizations can respond efficiently and effectively, minimizing the impact on critical business operations.
- **Vendor and Partner Coordination:** Collaboration with external parties plays a significant role in maintaining operational continuity. Establishing clear communication channels and protocols with vendors and partners ensures their support during disruptions. This alignment with ASL objectives ensures that external support is geared toward maintaining critical business operations and meeting defined availability and recovery objectives.

 Copyright © [2023] BRCCI (brcci.org)

Section 6.5.2 - Level B: IT Services

At this level, the objective is to develop resiliency strategies for the IT infrastructure and services that support an organization's day-to-day operations. These services encompass everything from data management to application support, and they are critical to ensuring seamless business processes and customer experiences. The development of resiliency strategies includes considerations for the following aspects of IT services:

- Redundancy and Failover Systems: To ensure uninterrupted service, organizations should implement redundant IT systems. These systems act as backups, ready to take over if the primary system encounters issues. Coupled with failover mechanisms, this approach helps meet ASL targets for service uptime, response times, and recovery points, safeguarding against potential service interruptions.

- Data Backup and Recovery: Data is a cornerstone of IT services, and its protection is a vital objective of resiliency strategy. Organizations need robust backup and recovery procedures that align with ASL requirements. These procedures ensure data resilience, minimizing the risk of data loss and ensuring recovery within the acceptable time frame in the event of system failures or data corruption.

- Performance Monitoring and Optimization: Continuous monitoring of IT service performance is needed to maintain acceptable service levels. By tracking key performance indicators (KPIs), potential issues can be identified and addressed proactively. This proactive approach helps meet ASL targets for service availability and response times.

- Incident Response Plans: Specific incident response plans for IT services are a crucial part of the resiliency strategy. These plans should be designed with ASL objectives in mind, outlining procedures for rapid incident detection, containment, and resolution. With a well-defined response strategy, IT-related incidents are managed efficiently, and their impact on service availability is minimized.

- Vendor Management: IT service continuity requires an effective strategy for vendor management. The resiliency strategy includes an objective to achieve ASL targets by maintaining strong relationships with vendors. This ensures timely support and resolution of IT-related issues, reducing downtime and potential service disruptions. Regular communication and performance reviews with vendors help to maintain alignment with ASL objectives and organizational expectations.

Section 6.5.3 - Level C: Cloud Environment

The cloud environment presents both benefits and challenges for resiliency management. The resiliency strategy leverages the benefits of cloud technology while ensuring the resilience and stability necessary to meet Acceptable Stability Levels (ASL). The following aspects of the cloud environment should be considered for resiliency strategy development:

 Copyright © [2023] BRCCI (brcci.org)

Service Level Agreements (SLAs):

Resiliency requires clear and well-defined SLAs with cloud service providers. These agreements should outline specific ASL targets related to service availability, performance, and support. Aligning SLAs with resiliency objectives is essential for the consistent performance and reliability of cloud services.

Data Security and Compliance:

Security remains a major concern in the cloud environment. Implementation of a resilient data security strategy safeguards data integrity and confidentiality. Additionally, maintaining regulatory obligations and compliance related to data security is a key objective for cloud resiliency.

Backup and Redundancy:

The cloud environment inherently offers advantages in backup and redundancy. Implementing these measures within the cloud environment is essential to ensure data resilience and availability. Organizations can minimize disruptions during service outages or disruptions with effective backup strategies, effectively meeting ASL requirements.

Cloud resiliency strategy should span across various levels of infrastructure and services.

- Infrastructure Level: At the foundational level, cloud providers often offer redundant hardware setups, ensuring that physical servers and storage devices have backup counterparts. This hardware redundancy minimizes the risk of hardware failures causing service interruptions.
- Platform Level: Platforms within the cloud, such as databases or application hosting services, also integrate backup mechanisms. Automated backups and snapshots are commonly provided features that allow organizations to restore their data and configurations swiftly in case of errors or data corruption.
- Service Level: Beyond infrastructure and platform layers, individual services and applications also benefit from redundancy. Load balancing across multiple instances ensures that if one instance fails, traffic is seamlessly redirected to others, maintaining service availability.

Performance Monitoring and Optimization:

For a cloud environment, performance monitoring is not a one-time task but a continuous process. It's part of a proactive resiliency strategy that helps stay ahead of potential challenges and ensures optimal service delivery. The resilience strategy should consider its application. Here's an in-depth look at this critical aspect:

 Copyright © [2023] BRCCI (brcci.org)

- Continuous Monitoring:
  Monitor cloud service performance regularly. By consistently tracking key performance indicators (KPIs), insights are gained into system health, responsiveness, and overall efficiency. This ongoing monitoring allows prompt detection of deviations from expected normal operations and performance.

- Alert Mechanisms:
  Implement robust alert systems for immediate notifications of any performance anomalies or issues. A proactive alerting mechanism enables efficient responses, reducing the time to identify and address potential problems.

- Root Cause Analysis:
  Beyond mere detection, root cause analysis helps to understand the root cause of detected performance issues. Thorough root cause analyses (RCAs) pinpoint underlying issues, facilitating effective resolution and preventing recurrence.

- Resource Optimization:
  Cloud environments offer flexibility in resource allocation. By analyzing performance metrics, resource utilization is optimized, ensuring neither underutilization nor overprovisioning. This optimization enhances performance while also optimizing costs.

- Adaptive Scaling:
  Leveraging the cloud's elasticity, adaptive scaling allows for the dynamic adjustment of resources based on demand. Through an auto-scaling capability, optimal performance is achieved during peak loads while optimizing costs during low-demand periods.

- Performance Tuning:
  Regular tuning of the cloud environment should be based on performance insights. Performance tuning helps achieve consistent and improved service levels. Whether optimizing database queries, fine-tuning application configurations, or adjusting network parameters, these tweaks or tuning lead to a smoother, more efficient, and resilient operation.

SECTION 6.6 – S6: SKILLS-STRATEGY GAP ASSESSMENT (SGA)

This stage (S6) requires a Skills-Strategy gap assessment, which identifies the gap between existing skills and capabilities and those required by the strategies selected in the preceding stage (S5). The scope of the assessment includes the three core levels as mentioned in S2 – Resiliency Risk Management stage:

- Level A - Critical Business Operations
- Level B - IT Services
- Level C - Cloud Environment

 Copyright © [2023] BRCCI (brcci.org)

For each of the three core levels, the Skills-Strategy Gap assessment is approached with consideration for the following operational phases:

Normal Phase: During this phase, an assessment is conducted to evaluate the existing in-house skills and expertise relevant to maintaining the continuous stability of operations and services under normal operational conditions. This assessment identifies gaps between the current skill set and the requirements outlined by the resiliency strategy. Strategies are devised to bridge identified gaps, which may include training programs, skill development initiatives, or recruitment efforts to augment existing capabilities.

Prevention Phase: Preceding the onset of potential disasters, proactive measures are taken to prevent or minimize the likelihood of disruptions. An assessment of existing in-house skills is conducted to determine their adequacy in implementing preventive strategies outlined by the resiliency strategy. Any gaps identified are addressed through targeted strategies that enhance capabilities related to risk identification, vulnerability assessment, and preemptive mitigation measures.

Response Phase: In the event of a disaster, immediate actions are imperative to stabilize and mitigate the impact of disruptions. An assessment is conducted to evaluate the existing in-house skills and expertise relevant to executing response strategies outlined by the resiliency strategy. Any gaps identified are addressed through rapid training programs, skill mobilization efforts, or collaboration with external experts to ensure a swift and effective response to emergent challenges.

Recovery Phase: Following the initial response to stabilize disruptions, efforts are directed toward recovering normal operations. An assessment is conducted to evaluate the existing in-house skills and expertise required for executing recovery strategies outlined by the resiliency strategy. Identified gaps are addressed through targeted initiatives to restore critical functions, rebuild infrastructure, and facilitate business continuity.

Once the gap is assessed, the next step is to develop an alignment strategy to align the skills and capabilities required to achieve the resiliency strategy. The alignment strategy also determines the balance of in-house and outsourced skills and capabilities. A significant Skills-Strategy gap may require changes or modifications in the resiliency strategy to reduce the gap to an acceptable level.

SECTION 6.7 – S7: PLAN DESIGN AND DEVELOPMENT

The objective in the seventh stage is to develop the Business Continuity and Resiliency (BCR) plan documents, utilizing the strategies devised in Stage Five and aligning with the skills and capabilities identified in Stage Six. The BCR plans to serve as comprehensive guidance documents aimed at maintaining Acceptable Stability Levels (ASL) across the following four operational phases:

 Copyright © [2023] BRCCI (brcci.org)

- Normal Phase: These plans contain guidance to ensure the continuous stability of operations and services during routine operational conditions. This includes measures to ensure seamless operations, effective incident management, and coordination with vendors and cloud service providers.
- Prevention Phase: BCR plans offer guidance to preemptively prevent or minimize the likelihood of disruptions. They encompass proactive measures and protocols designed to identify and address potential risks and vulnerabilities before they escalate into significant disruptions.
- Response Phase: In the event of a disaster, BCR plans to outline immediate response actions to stabilize and mitigate the impact of disruptions. These plans include predefined procedures for activating emergency response teams, initiating crisis communication protocols, and mobilizing resources for effective incident management.
- Recovery Phase: Following the initial response to stabilize disruptions, BCR plans guide the recovery and restoration of the business environment. The plans outline strategies and procedures to expedite the recovery process, restore critical functions and services, and facilitate the transition back to normal operations or a new operational environment.

The guidance and procedures outlined in BCR plans are aligned with the constraints and dependencies identified in Stage Four.

For effective management and organization, BCR plans can be structured according to the three core levels identified in the Resiliency Risk Management stage (S2):

Level A - Business Operations: The Business Resiliency Plan document outlines strategies and procedures for maintaining the continuity and resilience of critical business operations.

Level B - IT Services: The IT Resiliency Plan document focuses on strategies and procedures to maintain the continuity and resilience of IT services and infrastructure.

Level C - Cloud Environment: The Cloud Resiliency Plan document addresses resilience strategies and procedures specific to cloud-based services and infrastructure.

These plans provide comprehensive guidance and procedures tailored to maintain Acceptable Stability Levels (ASL) across all operational phases, ensuring the organization's commitment to continuous resiliency. They detail specific actions to be taken, the resources required, and the individuals responsible for executing the plans, facilitating a coordinated and effective response to disruptions at all levels of the organization.

SECTION 6.8 – S8: MONITORING AND TESTING

This stage consists of two Processes: Monitoring and Testing.

 Copyright © [2023] BRCCI (brcci.org)

Monitoring is a continuous process to look-out for gaps and weaknesses that may disrupt Acceptable Stability Levels (ASL) across all operational phases. It ensures the organization's commitment to continuous resiliency. During normal conditions, monitoring is pivotal for maintaining and regulating the stability of business operations, IT services, and the cloud environment. In times of disaster, monitoring becomes even more crucial, overseeing and managing the stability of the disaster recovery process for a prompt and effective response.

Testing is a process that helps to evaluate and enhance resiliency strategies and plans. It consists of two distinct modes of evaluation: Change Management Resiliency (CMR) Testing and Disaster Management Resiliency (DMR) Testing.

Change Management Resiliency (CMR) Testing is active during normal conditions, focusing on assessing significant modifications and changes planned that may impact business operations, IT services, and the cloud environment. The objective is to verify that these changes do not compromise Acceptable Stability Levels (ASL). The CRM testing may require creating a sandbox environment to evaluate the feasibility of changes and their impact on the ASL of the existing production environment.

Disaster Management Resiliency (DMR) Testing is useful for validation and refinement of Business Continuity and Resiliency (BCR) plans, with the objective of assessing their effectiveness and practicality in real-world scenarios. This includes tabletop exercises, simulations, and full-scale tests aimed at assessing the organization's readiness and capability to execute plans seamlessly across all operational phases. Through testing and validation, gaps, weaknesses, and areas for improvement within the plans are identified.

SECTION 7.0 – CORE COMPONENT: RESILIENCY PROGRAM MANAGEMENT

The previous section described the resiliency planning process as Segment A of the ICR architecture. The core component, Segment B, provides a framework for the management of the resiliency planning process. This framework includes 10 management functions.

Section 7.1 - F1: Resiliency objective Management

The resiliency objectives form the guiding framework for the organization's resiliency program. They provide a roadmap through which all processes and activities within the program are aligned to achieve the overall resilience goals. The process of formulating resiliency objectives consists of the following essential steps to achieve clarity, relevance, and alignment with organizational needs:

1. Understanding the Context of the Organization
2. Assessing resiliency scope
3. Establishing Resiliency Objectives

 Copyright © [2023] BRCCI (brcci.org)

Resiliency objectives are foundational to the organization's resiliency program, providing a structured framework for its development and implementation. These objectives act as a guiding compass, directing all efforts and initiatives within the program toward achieving overarching resilience goals. The process of formulating resiliency objectives involves several essential steps to ensure clarity, relevance, and alignment with organizational needs:

Section 7.1.1 - Understanding the Context

Understanding the Context of the Organization: Before defining resiliency objectives, it is important to understand and assess the organization's internal and external context. This assessment process can occur at several levels across the organization including corporate, resilience posture, and stakeholders and regulatory levels.

At the corporate level, the process identifies all information that can give an idea of how the organization operates. It considers the organization's mission and vision, strategic goals, customer base, services, products, partnerships, and external obligations and relationships.

After conducting a corporate-level assessment, the next step is to understand the organization's resilience posture. This includes determining which areas of the business, IT, and cloud environment are critical and which threats pose a risk to resiliency.

The next step is to engage stakeholders and adhere to regulations. Organizations must identify stakeholders and relevant regulations to assess stakeholder expectations and regulatory requirements.

Section 7.1.2 - Assessing Resiliency Scope

After gaining insights into the organization's context and strategic priorities, the next step is to assess the scope for Integrated Continuous Resiliency. The scope defines the boundaries within which resiliency efforts will operate, such as organizational coverage and threat landscape:

Organizational Coverage: What areas and aspects of the organization should be covered by the resiliency program?

Threat Landscape: What are the types of risk conditions, incidents, and events should be managed by the resiliency program?

Organizational Coverage

Organizational coverage defines the scope by identifying the essential areas and aspects of the organization that the resiliency program should encompass and why they should be a part of the scope. The scope should be identified for each of the following organizational coverage categories:

1. Company branches and operational units
2. Customer segments

 Copyright © [2023] BRCCI (brcci.org)

3. Products and services
4. Business partners
5. Personnel and Resources
6. Facilities and infrastructure
7. Regulations and contractual obligations

Threat Landscape

Evaluating the threat landscape involves identifying the types of risk conditions, incidents, and events that should be managed by the resiliency program. This includes:

1. Natural category: This encompasses threats such as earthquakes, floods, hurricanes, and other natural disasters that could disrupt organizational operations.
2. Technical category: Cyber-attacks, system failures, data breaches, and other technical incidents pose significant risks to IT infrastructure and information assets.
3. People-related category: Human errors, sabotage, labor strikes, and other people-related incidents can impact organizational resilience and continuity efforts.

Section 7.1.3 - Establishing Resiliency Objectives

Building upon the insights gained from contextual analysis and scope assessment, the next step in the process is to establish specific resiliency objectives. These objectives are essential for guiding the organization toward maintaining stability and continuity across business, IT, and cloud functions and services, under all operating conditions.

The following definition of a general resiliency objective should guide the specific objectives:

> **"The objective is to maintain stability and continuity of the business, IT, and Cloud functions and service under all operating conditions by resisting and recovering from disruptive scenarios, incidents, and events."**

The specific objectives should be SMART (Specific, Measurable, Achievable, Relevant, Time-bound) and aligned with the organization's strategic priorities and risk tolerance. Whether focusing on minimizing downtime, enhancing data protection, or improving response capabilities, resiliency objectives should reflect the organization's commitment to resilience.

An integral part of defining resiliency objectives is assessing the acceptable stability levels (ASL) required to maintain operational continuity under varying conditions. ASL serves as a SMART performance metric to evaluate the organization's resilience capabilities across business, IT, and

 Copyright © [2023] BRCCI (brcci.org)

cloud environments. The parameters of ASL may include service availability, response times, recovery objectives, and overall performance.

Section 7.2 - F2: Personnel and Resource Management

The role of this management function is to provide oversight and coordination of personnel and assets to support the objectives and activities of the BCR program. This management function is performed in coordination with stage 6 (Skills-Strategy Gap Assessment) of the resiliency planning process.

The effectiveness of a BCR program relies on a coordinated effort from all stakeholders, including senior management, employees, customers, suppliers, and external partners. Through this coordination, the personnel and resource management function defines roles and responsibilities, develops a competent and trained workforce, and manages resources and infrastructure.

- Defining Roles and Responsibilities: Clearly defining the roles and responsibilities of each stakeholder enables accountability and clarity in executing resiliency plans. The Personnel and Resource Management function identifies and defines the roles and responsibilities of all key personnel who will be responsible for various aspects of the BCR program.
- Developing a Competent and Trained Workforce: A competent and trained workforce is essential for maintaining operational stability and continuity. The Personnel and Resource Management function should be responsible for ongoing training and development programs to enhance the resiliency-related competency and capabilities of personnel across all levels of the organization.
- Managing Resources and Infrastructure: The effectiveness of a resiliency program relies on the timely availability of adequate resources and infrastructure. The Personnel and Resource Management function manages physical resources such as technology systems, equipment, and facilities, as well as financial resources to fund resiliency initiatives and investments in infrastructure upgrades. The management function also performs regular assessments of resource requirements and availability.

Section 7.3 - F3: Incident Resiliency Management

Traditionally, incident management functions and business continuity processes operate in silos within many organizations. These silos can create communication gaps, inefficiencies, and inconsistencies in response efforts. However, the BCR program breaks down these barriers by integrating the incident management function as a core component of its resiliency architecture. This integration ensures a cohesive and streamlined approach to incident response, eliminating silos and fostering collaboration across functions.

As an integral component of the Business Continuity and Resiliency (BCR) program, Incident Resiliency Management (IRM) deals with two key categories of incidents. The first

 Copyright © [2023] BRCCI (brcci.org)

category is related to minor incidents that can disrupt business functions and operations, while the second category is specific to incidents related to the IT and Cloud computing environment.

A proactive IRM approach is essential for managing minor incidents that can disrupt business operations. The BCR program should establish clear protocols and escalation pathways to promptly identify, assess, and respond to these incidents. Through robust incident management procedures, Incident Resiliency Management (IRM) aims to minimize downtime, maintain service levels, and protect customer trust. Regular training and awareness programs should be conducted to equip personnel with the necessary skills and knowledge to manage minor incidents effectively.

Incidents related to IT and Cloud computing environments require specialized attention due to their potential to cause widespread disruption and data loss. The IRM function should provide incident response plans tailored to address the unique challenges posed by these incidents, including cybersecurity threats, data breaches, and service outages. The incident response effort should extend to collaboration and coordination with IT and Cloud service providers.

The IRM function tracks and monitors incidents proactively through a centralized incident tracking system, recording and monitoring incidents from identification to resolution. This system should capture key information such as incident type, impact, response actions taken, and lessons learned. The incident data should be regularly analyzed to identify trends, recurring issues, and areas for improvement.

In line with the concepts of continuous resiliency and Acceptable Stability Levels (ASL), the BCR program should continuously assess the effectiveness of its incident management strategies. Regular reviews, simulations, and audits should be conducted to test the organization's preparedness and identify areas for enhancement.

Section 7.4 – F4: Resiliency Plan Maintenance

Resiliency plans are a key deliverable of the BCR program and need consistent care and attention to remain effective. After developing, testing, and confirming their efficacy, these plans require regular updates to stay relevant and functional.

The insights from the function “F4 - Incident Resiliency Management” provide valuable data for plan maintenance. By tracking and analyzing incidents from both minor disruptions and those related to IT and Cloud computing environments, this data offers a real-world view of how our plans are performing. If certain incidents occur frequently or if patterns emerge, it signals areas in the plans that might need adjustment. Thus, the incident management function acts as a feedback loop, highlighting areas for improvement and refinement of resiliency plans.

The "Monitoring and Testing" stage from the resiliency planning process further aids the maintenance function. It provides a structured process to evaluate plans against real-world scenarios, helping to pinpoint areas of strength and potential weaknesses.

 Copyright © [2023] BRCCI (brcci.org)

Because organizations in today's business environment experience constant changes, both internally and externally, plans must adapt to those changes rapidly. Whether it's technological advancements, regulatory changes, or shifts in business strategies, these factors can impact plan effectiveness. The BCR program should conduct regular reviews to ensure plans evolve with these changes while remaining aligned with the resiliency objectives.

Section 7.5 – F5: Program Documentation Management

Program document management is a systematic and organized process for handling various documents and records used in or produced by a business resiliency program. This process manages documents and records related to the various stages of the resiliency planning process and functions of the resiliency program management.

A documentation management process ensures that vital information is organized, accessible, and up to date throughout the program's lifecycle. A key aspect of this process is the identification and classification of documents. This process pinpoints and categorizes essential documents, such as plans, policies, and contact lists, to ensure they are readily available when needed. Alongside this, the document management process should maintain document version control. By tracking revisions and updates, version control always provides access to the most current information, reducing confusion and potential errors.

Determining where and how documents are stored is equally important. Digital Document Management Systems (DMS) can be employed to securely store electronic files, while physical documents are safeguarded in inaccessible and secured locations.

The document management process should include access controls that only allow authorized individuals access to view and modify specific documents, maintaining confidentiality and integrity. The access control should include protocols for timely retrieval and distribution of documents during a disruptive event.

In addition, the document management process must adhere to the following requirements:

- Comply with legal and regulatory requirements, as well as industry standards and best practices.
- Establish a governance framework for documentation that sets clear roles and responsibilities for managing the document lifecycle.
- Establish the appropriate disposal methods for outdated or unnecessary documents.

Section 7.6 – F6: Plans Integration and Rollout

The integration and rollout of the Business Continuity and Resiliency (BCR) program are a pivotal process to embed resilience across the organization. For a smooth and effective transition, it's essential to have a structured rollout and integration plan. This section elaborates on the necessity of these plans and their components.

 Copyright © [2023] BRCCI (brcci.org)

Integration: Integration is a multifaceted process conducted at two levels to embed the BCR program across the organization.

First Level Integration: At this level, the BCR program is aligned with the organization's culture, objectives, and strategic goals. The integration plan should identify gaps or overlaps with existing systems and develop strategies to bridge them. It should also outline the steps to integrate ASL as a key metric in the organization's resilience framework.

Second Level Integration: At this second level, resiliency plans are consolidated from various parts of the organization into a unified BCR program. The integration plan for this level should specify how to harmonize different plans, standardize processes, and maintain consistency across the organization. It should also detail how ASL will be maintained or improved through this consolidation.

Rollout: The Rollout function is about introducing the BCR program comprehensively to all organizational levels. A well-defined rollout plan guides everyone in the understanding of their roles and responsibilities. This plan should outline the communication strategies, training modules, and timelines for the program's implementation. An integral part of this plan is the objective to maintain Acceptable Stability Levels (ASL) during and after the rollout. This prevents the rollout process itself from introducing vulnerabilities or disruptions.

Key Components of Rollout and Integration Plan:

- **Communication Strategy:** Define how information about the BCR program will be communicated across the organization.
- **Training Modules:** Develop training programs to educate employees about their roles and responsibilities.
- **Timeline:** Establish a timeline for the rollout and integration process, including key milestones and deadlines.
- **ASL Maintenance:** Clearly outline strategies and measures to maintain or improve Acceptable Stability Levels throughout the rollout and integration phases.
- **Monitoring and Evaluation:** Implement mechanisms to monitor the progress of the rollout and integration and evaluate their effectiveness.
- **Stakeholder Engagement:** Engage with key stakeholders to gather feedback and address concerns throughout the process.
- **Contingency Plans:** Develop contingency plans to address any challenges or disruptions that may arise during the rollout and integration.

 Copyright © [2023] BRCCI (brcci.org)

Section 7.7 – F7: Program communication and coordination

An efficient communication and coordination strategy is critical to the success of the Business Continuity and Resiliency (BCR) program. In responding to disruptions or incidents, the effectiveness of resiliency plans depends on the clarity of communication. The clarity of communication allows everyone to be well-informed and respond timely and effectively.

In addition to clarity, strong and transparent communication prevents misunderstandings, confusion, and the potential for errors. Effective communication and coordination are instrumental to the program's integrity and reliability.

Internally, communication and coordination procedures should be established to ensure stakeholders are aware of their roles and responsibilities related to the BCR program. These procedures establish clear lines of communication between different teams or departments, create communication protocols, and establish regular communication channels to keep stakeholders informed of any changes or updates to the program.

Externally, communication and coordination procedures should exist to interact with external partners, suppliers, and stakeholders involved in the BCR program and incident response efforts. These procedures establish communication protocols with external parties, such as emergency services, vendors, or regulators, fostering effective collaboration and information exchange.

Section 7.8 – F8: Continual Program Improvement

Continual Program Improvement is a foundational principle of the ICR standard, focusing on enhancing the business resiliency program in three main areas: Program Maturity, Resiliency Culture, and Quality Assurance.

Section 7.8.1 – Program Maturity Improvement

Advancing program maturity means gradually evolving the business resiliency program to higher levels of effectiveness and efficiency. The resiliency program should continually adapt to ever-changing organizational needs and external factors.

Key elements guiding this maturity process include:

- **Incremental Improvement:** Business resiliency isn't static; it is constantly evolving. Emphasizing gradual enhancement allows the program to adjust to new challenges without causing major disruptions.
- **Program Assessment:** Routine evaluations are vital. They should cover all aspects of the program, from risk assessments to recovery strategies, helping to identify areas needing attention.

 Copyright © [2023] BRCCI (brcci.org)

- **Adjustments and Adaptations:** Once areas for improvement are pinpointed, necessary changes should be implemented promptly. This might mean updating protocols or integrating new technologies.
- **Strategic Planning:** Advancing program maturity requires clear goals and milestones. These should be set in line with organizational risk tolerance, ensuring they align with broader business objectives.
- **Feedback Mechanisms:** Open channels for feedback ensure the program remains aligned with organizational goals. This input can come from incident reviews, simulations, or regular discussions.
- **Documentation and Reporting:** Maintaining thorough documentation and regular reporting provides insights into the program's progress, helping guide future improvements.

Section 7.8.2 – Resiliency Culture Development

The success of a resiliency program depends on how effectively continuity and resiliency is embedded in the organization's culture. The most successful resiliency plans are those that have extensive awareness, involvement, and commitment from everyone in the organization.

The resiliency culture development is a continual process that instills a shared understanding and commitment to resiliency principles across all levels of the organization, from frontline employees to senior leadership. This continual process incrementally aligns the resiliency culture with the program's maturity.

Every activity and project within the resiliency program should be considered an opportunity to improve the level of resiliency culture. Encouraging a sense of ownership and accountability among employees is key. Recognition and rewards can further motivate behaviors that bolster organizational resilience.

The culture development process includes the following steps:

1. Identify requirements: As a first step, understand the level of awareness of the resiliency program within the organization. Identify the specific needs and challenges of the organization regarding the development of a resiliency culture. Document current cultural strengths, weaknesses, and areas for improvement.
2. Define objectives: Establish clear and measurable objectives for enhancing resiliency culture based on the requirements in Step 1. These objectives should align with the overall goals and activities of the resiliency program.
3. Implement measures: Implement targeted measures and initiatives to achieve the objective of Step 2. These measures consist of training and awareness programs,

 Copyright © [2023] BRCCI (brcci.org)

resiliency leadership development initiatives, communication strategies, and embedding resiliency principles into everyday practices and processes.

4. Foster collaboration and communication: Promote open communication and collaboration across all levels of the organization to promote a shared understanding of resiliency goals and objectives. Encourage feedback, ideas, and contributions from employees to continuously improve the resiliency culture.

5. Monitor and evaluate progress: Regularly monitor and evaluate progress toward achieving resiliency culture objectives. Collect feedback from employees, assess the effectiveness of implemented measures, and adjust strategies to address any emerging challenges or opportunities.

Section 7.8.3 – Program Quality Assurance

Program Quality Assurance fortifies organizational resilience against disruptions and challenges. As a holistic approach, it aligns all aspects of the resiliency program with organizational objectives and industry standards. At its core, Program Quality Assurance instills confidence in the organization's ability to remain resilient to disruptions and instabilities under all operating scenarios.

An integral part of Program Quality Assurance is the establishment of robust governance structures and processes to oversee resiliency initiatives. Governance refers to the overarching framework of policies, procedures, and mechanisms put in place to guide and oversee resiliency initiatives across the organization. At its core, governance ensures that resiliency efforts are aligned with organizational objectives, regulatory requirements, and industry standards.

Key components of Program Quality Assurance in the ICR framework include:

- Policy and Procedure Development: Well-defined and regularly updated policies and procedures serve as the cornerstone of effective resiliency management within the organization. These documents outline the strategies and protocols to be followed during times of disruption or crisis.

- Documentation and Plan Review: Regular reviews and version controls are essential to maintain the accuracy and relevance of resiliency plans. By continuously assessing and updating these documents, organizations can ensure readiness and responsiveness to evolving threats and challenges.

- Testing and Exercises: Routine testing and simulation exercises are conducted to validate the effectiveness of resiliency plans and procedures. These exercises provide invaluable insights into areas of strength and weakness, facilitating targeted improvements and enhancements.

- Audit Processes: Internal audits and potentially external assessments are conducted to verify compliance with organizational and industry standards. These audits serve as a

 Copyright © [2023] BRCCI (brcci.org)

mechanism to identify gaps and areas for improvement, driving ongoing refinement of the resiliency program.

- Regulatory Compliance: Ensuring adherence to relevant regulations and standards is paramount for organizational resilience. This component involves aligning resiliency initiatives with regulatory requirements and incorporating compliance measures into program activities and processes.
- Key Performance Indicators (KPIs): Metrics such as recovery time objectives (RTO) and recovery point objectives (RPO) are utilized to measure the performance and efficacy of resiliency efforts. These KPIs provide quantifiable benchmarks for evaluating the program's effectiveness and efficiency.
- Continual Improvement: Incident analysis and audit findings are leveraged to identify lessons learned and opportunities for enhancement. By embracing a culture of continual improvement, organizations can adapt and evolve their resiliency strategies to address emerging threats and challenges effectively.
- Training and Awareness: Ongoing training and awareness initiatives ensure that all stakeholders are equipped with the necessary knowledge and skills to contribute effectively to resiliency efforts. By fostering a culture of awareness and preparedness, organizations can enhance their overall resilience posture.
- Change Management: A robust change management process is essential to evaluate the impact of any alterations on resiliency capabilities. By systematically assessing and managing changes, organizations can minimize disruptions and maintain continuity in the face of evolving circumstances.
- Supplier and Third-Party Management: Evaluating the resilience of critical suppliers and incorporating resiliency requirements into contracts are integral aspects of program quality assurance. By extending resiliency considerations to external partners and vendors, organizations can mitigate risks and strengthen the overall resilience of their supply chain.

SECTION 8.0 – AUDIENCE

The ICR Implementation Reference Standard is intended for a wide range of stakeholders involved in the development, implementation, and maintenance of BCR programs, including:

- Senior management and executive leaders responsible for setting the strategic direction and priorities of the organization.
- Business continuity and resiliency professionals responsible for designing, implementing, and maintaining BCR programs.

 Copyright © [2023] BRCCI (brcci.org)

- Risk management professionals responsible for identifying, assessing, and mitigating risks that could disrupt business operations.
- IT professionals responsible for ensuring the availability and resilience of critical systems, applications, and infrastructure.
- Human resources professionals responsible for employee training, awareness, and support in the context of BCR.
- Operations and supply chain management professionals responsible for ensuring the continuity and resilience of critical business processes and supply chains.

SECTION 9.0 – TERMS AND DEFINITIONS

This section contains a list of essential terms and definitions used or referenced in the ICR standard. It is recommended that users familiarize themselves with the definitions provided herein to facilitate discussions, planning, and implementation of resilience initiatives in accordance with the ICR standard.

Integrated Continuous Resiliency (ICR) Standard: A comprehensive framework developed by BRCCI for continuity and resiliency best practices, offering organizations a unified approach to achieve continuity and resiliency across business functions, IT services, and Cloud environments.

- **Resiliency:** The capability to maintain operational stability and service reliability across all levels of an organization under normal and disaster conditions.
- **Integrated Resiliency:** Emphasizes the importance of permeating resiliency across all levels of an organization, integrating resilience at every level from core business functions to IT systems and cloud services.
- **Continuous Resiliency:** Focuses on maintaining operational stability and service reliability at all times, irrespective of disaster scenarios, ensuring readiness to face disruptions ranging from minor to full-scale crises.
- **Business Continuity and Resiliency (BCR) Program:** An organizational framework aimed at achieving resiliency across all levels, continuously, and under all operating conditions.
- **Business Continuity (BC) Program:** An initiative focused on maintaining operational continuity in the event of disruptions or disasters.
- **IT Disaster Recovery (IT DR) Program:** A set of procedures and policies aimed at recovering IT systems and data after a disaster.

 Copyright © [2023] BRCCI (brcci.org)

- **Cloud Recovery Plan:** Strategies and protocols for recovering cloud-based services and data in the event of a disruption or disaster.
- **Program Definition:** The articulation of objectives and scope for the business continuity and resiliency program, expanding traditional BC and IT DR program objectives to include integrated operational stability under all operating conditions.
- **Program Architecture:** The structural framework of the business continuity and resiliency program, emphasizing the separation of program management components and planning processes to delineate resiliency objectives at various levels.
- **Business-Technology Interface:** The nexus between business and technology resilience within the program planning process, encompassing stages such as Business Impact Assessment (BIA), Constraints and Dependencies Management, Skills-Strategy Gap Assessment, and Monitoring and Testing.
- **Resiliency Objective:** The overarching goal of maintaining acceptable stability levels (ASL) during both normal and disaster periods.
- **Resiliency Planning Process:** A lifecycle consisting of stages such as Resiliency Process Definition, Resiliency Risk Management, Business Impact Analysis (BIA), Constraints and Dependencies Management, Resiliency Strategy Development, Skills-strategy Gap Assessment, Plan Design and Development, and Monitoring and Testing.
- **Resiliency Program Management:** The management of the resiliency planning process, involving functions such as Resiliency Objective Management, Personnel and Resource Management, Incident Resiliency Management, Resiliency Plans Maintenance, Program Documentation Management, Plans Integration and Rollout, Program Communication and Coordination, and Continuous Program Improvement.
- **Acceptable Stability Levels (ASL):** Defined thresholds for stability and service reliability during both normal operational conditions and disaster scenarios.
- **Segment A:** The section of the ICR architecture that defines the resiliency planning process, consisting of 8 stages.
- **Stage S1: Resiliency Process Definition:** The initial stage of the resiliency planning process, defining objectives, scope, constraints, and interdependencies for subsequent stages of the BCR lifecycle.
- **Stage S2: Resiliency Risk Management:** The stage focused on assessing and managing risks to ASL across three core levels: business operations, IT services, and Cloud environment.

 Copyright © [2023] BRCCI (brcci.org)

- **Stage S3: Business Impact Analysis (BIA):** A stage aimed at understanding the potential impacts of disruptions on critical business functions and identifying requirements for recovery.
- **Stage S4: Constraints and Dependencies Management:** A stage addressing effective management of factors such as supply chain dependencies, resource limits, and regulatory obligations to maintain ASL.
- **Stage S5: Resiliency Strategy Development:** A stage providing strategies and solutions to satisfy BCR program requirements and maintain ASL across various operational phases.
- **Stage S6: Skills-Strategy Gap Assessment (SGA):** A stage assessing the gap between existing skills and capabilities and those required by resiliency strategies, with a focus on bridging these gaps to achieve ASL.
- **Level A - Critical Business Operations:** The core level focuses on safeguarding critical business functions and operations essential for revenue streams, customer satisfaction, and organizational reputation.
- **Level B - IT Services:** The core level addresses resiliency strategies for IT infrastructure and services supporting day-to-day operations, including data management and application support.
- **Level C - Cloud Environment:** The core level deals with resiliency strategies specific to cloud technology, leveraging benefits while ensuring stability and resilience to meet ASL.
- **Business Continuity and Resiliency (BCR) Plan Documents:** Comprehensive guidance documents developed in Stage Seven, outlining strategies and procedures to maintain Acceptable Stability Levels (ASL) across various operational phases.
- **Normal Phase:** Operational conditions where BCR plans aim to ensure continuous stability, seamless operations, effective incident management, and coordination with vendors and cloud service providers.
- **Prevention Phase:** Operational phase where BCR plans to focus on preemptively preventing or minimizing disruptions through proactive measures and protocols.
- **Response Phase:** Operational phase where BCR plans outline immediate response actions to stabilize and mitigate the impact of disruptions, including activating emergency response teams and crisis communication protocols.
- **Recovery Phase:** Operational phase following the initial response to stabilize disruptions, where BCR plans guide the recovery and restoration of the business environment.
- **Level A - Business Operations:** Core level focusing on strategies and procedures for maintaining the continuity and resilience of critical business operations.

 Copyright © [2023] BRCCI (brcci.org)

- **Level B - IT Services:** Core level addressing strategies and procedures to maintain the continuity and resilience of IT services and infrastructure.
- **Level C - Cloud Environment:** Core level addressing resilience strategies and procedures specific to cloud-based services and infrastructure.
- **Monitoring:** Continuous process of observing and regulating stability across business operations, IT services, and the cloud environment to maintain ASL.
- **Testing:** Process of evaluating and enhancing resiliency strategies and plans, including Change Management Resiliency (CMR) Testing and Disaster Management Resiliency (DMR) Testing.
- **Change Management Resiliency (CMR) Testing:** Testing mode focusing on assessing significant modifications and changes planned to ensure they do not compromise ASL during normal conditions.
- **Disaster Management Resiliency (DMR) Testing:** Testing mode for validating and refining BCR plans, assessing their effectiveness and practicality in real-world scenarios, including tabletop exercises, simulations, and full-scale tests.
- **Resiliency Objectives:** Framework guiding the organization's resiliency program, aligning processes and activities to achieve overall resilience goals.
- **Understanding the Context:** Process of assessing the organization's internal and external context before defining resiliency objectives.
- **Assessing Resiliency Scope:** Process of defining the boundaries within which resiliency efforts will operate, including organizational coverage and threat landscape assessment.
- **Incident Resiliency Management (IRM):** Management function integrating incident management as a core component of the BCR program, dealing with minor incidents and IT/cloud-related incidents.
- **Resiliency Plan Maintenance:** Function responsible for the consistent upkeep and adaptation of resiliency plans to ensure relevance and effectiveness over time.
- **Program Documentation Management:** Process of systematically handling various documents and records used in or produced by a business resiliency program, ensuring accessibility, version control, and compliance.
- **Plans Integration and Rollout:** Process of embedding the BCR program across the organization through integration with existing systems and comprehensive rollout plans.

 Copyright © [2023] BRCCI (brcci.org)

- **Program Communication and Coordination:** Principles and procedures ensuring effective internal and external communication and coordination within the BCR program to preserve integrity and ensure success.
- **Continuous Program Improvement:** The ongoing process of enhancing the business resiliency program to adapt to changing organizational needs and external factors.
- **Program Maturity:** The level of effectiveness and efficiency reached by the business resiliency program over time.
- **Incremental Improvement:** Gradual enhancement of the business resiliency program without causing major disruptions.
- **Program Assessment:** Routine evaluations covering all aspects of the business resiliency program, from risk assessments to recovery strategies.
- **Adjustments and Adaptations:** Implementation of necessary changes identified through program assessment to improve the effectiveness of the resiliency program.
- **Strategic Planning:** Setting clear goals and milestones for advancing program maturity in alignment with organizational risk tolerance and broader business objectives.
- **Feedback Mechanisms:** Open channels for receiving feedback to ensure the resiliency program remains aligned with organizational goals.
- **Documentation and Reporting:** Maintaining thorough documentation and regular reporting to provide insights into the progress of the resiliency program.
- **Resiliency Culture Development:** The process of promoting awareness about continuity and fostering proactive risk management behaviors across all staff levels.
- **Ownership and Accountability:** Encouraging a sense of ownership and responsibility among employees for contributing to organizational resilience.
- **Recognition and Rewards:** Motivational strategies aimed at reinforcing behaviors that strengthen organizational resilience.
- **Program Quality Assurance:** The process of ensuring the reliability and effectiveness of business continuity and IT disaster recovery plans.
- **Policy and Procedure Development:** Creating clear and updated policies and procedures as the foundation of effective business continuity and IT disaster recovery efforts.
- **Documentation and Plan Review:** Regular reviews and version controls to keep business continuity and IT disaster recovery plans accurate and up-to-date.

 Copyright © [2023] BRCCI (brcci.org)

- **Testing and Exercises:** Routine tests and exercises to validate the effectiveness of business continuity and IT disaster recovery plans.
- **Audit Processes:** Internal and potentially external audits to ensure compliance with organizational and industry standards.
- **Key Performance Indicators (KPIs):** Metrics such as recovery time and point objectives (RTO/RPO) used to measure the performance of business continuity and IT disaster recovery efforts.
- **Continual Improvement:** A culture of ongoing enhancement and refinement of the BCR program based on feedback and lessons learned.
- **Change Management:** A process to track, control, and assess changes to business processes, IT systems, and infrastructure.
- **Supplier and Third-Party Management:** The assessment and monitoring of the resilience of critical suppliers and third-party service providers.
- **Acceptable Stability Levels (ASL):** A broader definition of resiliency objectives introduced by ICR standard, encapsulating both availability and continuity objectives across all operational states, both normal and during disaster scenarios.
- **BC (Business Continuity):** A traditional framework focusing on maintaining operational continuity during disaster situations.
- **BIA (Business Impact Analysis):** A process that identifies critical and non-critical business functions, assesses potential impacts of disruptions and identifies recovery requirements for critical functions during a disruption.
- **BCR (Business Continuity and Resiliency) Framework:** Structured around three key components: Program Definition, Program Architecture, and Business-Technology Interface. It advocates for functional separation between program management and planning processes.
- **Continuous Resiliency:** The principle of prioritizing operational stability at all times, including both normal conditions and disaster situations, as introduced by ICR.
- **Constraints and Dependencies:** Factors that may limit or impact the resiliency of an organization's operations, including supply chain dependencies and resource limitations.
- **Core Component:** The central part of the ICR architecture made up of 11 elements focusing on resiliency program management.
- **Continuous Resiliency:** A principle prioritizing operational stability at all times, including both normal conditions and disaster situations, as introduced by ICR.

 Copyright © [2023] BRCCI (brcci.org)

- **MTBF (Mean Time Between Failure):** A metric focusing on the average time between failures or disruptions in a system or process.
- **MTTR (Mean Time to Recovery):** A metric indicating the average time taken to restore a system or process after a failure or disruption.
- **MTTD (Mean Time to Detection):** A metric indicating the average time taken to detect a failure or disruption in a system or process.
- **MTDs (Maximum Tolerable Downtimes):** The maximum acceptable duration of time that a system or process can be down or unavailable without causing significant harm to an organization.
- **MTDDS (Maximum Tolerable Data Downtime and Loss):** The maximum amount of time and data an organization can afford to lose.
- **BCR Plans:** Detailed roadmaps that guide the organization on how to manage and recover critical functions during disruptions.
- **Monitoring:** Continuous surveillance for gaps and weaknesses in business operations and IT services.
- **Testing:** Activities aimed at assessing the impact of changes and validating the effectiveness of BCR plans.
- **Risk Appetite:** The level of risk an organization is willing to accept in pursuit of its objectives.
- **Incident:** An event that disrupts normal business operations and may require activation of BCR plans.
- **Risk Mitigation:** Actions taken to reduce the potential impact or likelihood of identified risks.
- **Document Management:** Systematic handling of documents and records essential for business continuity and resiliency.
- **Disaster Recovery and Backups:** Measures to safeguard critical documents and data from loss or damage.
- **Program-failure Risk Management:** A comprehensive approach to identifying, assessing, mitigating, and monitoring potential risks and vulnerabilities within a BCR program.
- **Rollout:** The process of introducing and implementing the BCR program to all relevant stakeholders.

 Copyright © [2023] BRCCI (brcci.org)

- **Integration:** The process of embedding the BCR program and plans into the organization's existing systems and processes.
- **Key Performance Indicators (KPIs):** Metrics used to measure the performance and effectiveness of BC and IT DR activities.
- **Resiliency Program Management:** A framework encompassing various management functions to guide the resiliency planning process.
- **Continual improvement:** The ongoing effort to enhance the effectiveness and efficiency of the BCR program over time.
- **Governance:** The framework of policies, procedures, and controls that guide and oversee the BCR program.
- **Incident Response:** Procedures and actions taken to address and mitigate the impact of incidents on business operations.
- **Communication:** Clear and effective communication is essential for ensuring a coordinated response to incidents and disruptions.
- **Coordination:** Collaboration and coordination among various stakeholders are crucial for the successful implementation of BCR plans.
- **Training and Awareness:** Training programs and awareness campaigns help ensure that all employees understand their roles and responsibilities in maintaining business continuity and resilience.
- **Testing and Exercises:** Regular testing and exercises are conducted to evaluate BCR plans' effectiveness and identify improvement areas.
- **Review and Audit:** Regular reviews and audits help ensure that BCR plans are kept up to date and in line with changing business needs and regulatory requirements.
- Program Evaluation: The process of assessing the overall effectiveness of the BCR program and identifying areas for improvement.

SECTION 10.0 – COPYRIGHT NOTICE AND PERMISSIONS

Copyright © [2023] by BRCCI. All rights reserved.

This document is a proprietary publication of BRCCI and is protected by copyright laws. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior

written permission of BRCCI, except as permitted under relevant copyright laws or by permission in writing from BRCCI.

While the use of this document's contents to implement the Integrated Continuous Resiliency (ICR) framework is protected by copyright, organizations, professionals, and practitioners in the field of business continuity and resiliency management are permitted to use this document to learn, apply, and implement the ICR framework within their respective organizations or client engagements.

However, any reproduction, adaptation, distribution, or other use of this document for commercial purposes, including but not limited to resale, licensing, or providing consulting services based on its content, requires the explicit written permission of BRCCI.

BRCCI makes no representations or warranties regarding the accuracy or completeness of the information in this document and shall not be liable for any direct, indirect, consequential, or incidental damages arising from the use or reliance upon the information provided herein.

For permission requests or further information, please contact BRCCI at info@brcci.org. To access this standard's latest information and version, visit brcci.org or brcci.org/standard.