kyndryl

September 2026

Business Continuity Management

Enterprise Position Paper



Contents

2 **Overview**

3 **Business Continuity Management and Governance**

3 Business Continuity Planning

3 Maintenance, Exercises, and Validation

4 **Frequently Asked Questions (FAQs)**

4 General Business Resiliency

5 Business Continuity Plans

6 Training, Exercising, and Maintenance

8 Recovery Strategy

8 Third-party Suppliers

Overview

Kyndryl recognizes that operational disruptions may impact its ability to deliver services to customers, support employees, and meet business obligations. To strengthen organizational resilience and support the continuity of critical operations, Kyndryl maintains a global Business Continuity Management (BCM) program designed to prepare for, respond to, and recover from disruptive events.

Kyndryl maintains Business Continuity Plans and supporting recovery procedures in accordance with its global enterprise policies, standards, and guidelines. These plans support the continued delivery and recovery of critical business operations through the assessment of business impacts, critical dependencies, and potential disruption scenarios.

Kyndryl defines Business Continuity as the organization's ability to maintain and recover critical operations during and following disruptive events. Such events may include natural disasters, cyberattacks, pandemics, power outages, civil unrest, and supply chain disruptions. Kyndryl follows industry-recognized practices and has invested in methodologies, tools, and governance frameworks to strengthen resilience across its global operations.

This paper provides an overview of Kyndryl's Business Continuity Management program, highlighting the strategies, processes, and controls used to prepare for, respond to, and recover from disruptions that could affect business operations.



Business Continuity Management and Governance

Kyndryl maintains a centralized Business Continuity Management System (BCMS) that provides a consistent framework, governance model, standards, and guidance across all Business Areas.

Corporate policies, standards, and guidelines establish the framework, and business areas implement these requirements to support the continuity and recovery of critical operations during natural, technological, or human-caused disruptions.

The framework is aligned with ISO 22301 and provides a structured approach for identifying and assessing business continuity risks, developing response and recovery strategies, documenting and maintaining continuity plans, conducting exercising activities, and understanding roles and responsibilities.

An Enterprise Business Continuity Management function provides enterprise-level oversight of business continuity preparedness, drives consistent implementation of BCMS requirements, and reports on resilience capabilities and program maturity to senior management.

Business Continuity Planning

Each Kyndryl Business Area is responsible for developing and executing its Business Continuity Plans and mitigation strategies. Kyndryl assesses a broad range of risks that could impact service delivery, company reputation, stakeholders, or personnel.

Critical business operations and processes are identified through the Business Impact Analysis (BIA) process, which evaluates the potential operational, financial, regulatory, contractual, customer, and reputational impacts of a disruption. For critical activities, Business Continuity Plans are developed and maintained to support the timely response and recovery of operations.

Critical business processes are supported by a range of technology assets, applications, and infrastructure. These supporting assets are assessed for criticality based on factors including regulatory requirements, contractual obligations, service level commitments, operational dependencies, and employee health and safety considerations.

To support business recovery objectives, critical technology assets are required to maintain appropriate data protection, backup, and disaster recovery capabilities aligned with the recovery requirements and criticality of the business processes they support. This helps ensure the availability and recoverability of essential services during disruptive events.

The CIO strategy prioritizes SaaS platforms and Hyperscalers and takes a modern operational approach, with multi-region deployment architecture and parallel processing as the standard for Kyndryl's CIO application portfolio rather than legacy on-premises solutions and off-site data retention.

Kyndryl systems achieve Recovery Time Objectives (RTO) through the use of stable, industry-proven solutions.

An integral component of Kyndryl's resilience is its Crisis Management capability. Crisis Management Teams (CMTs) are established at the corporate and regional levels, with governance and response capabilities designed to support all countries where Kyndryl delivers services. Crisis Management Teams, led by location leaders and representatives from key business functions, assess situations, direct response activities, support decision-making, coordinate stakeholder communications, and enable the continuity and recovery of critical business operations.

To support timely notification, escalation, and communication during incidents, Kyndryl utilizes the critical event management platform, enabling rapid dissemination of alerts, mobilization of response teams, and coordination of crisis management activities across the organization.

CMT preparedness is reinforced through regular training and exercises, with Crisis Management Teams conducting exercises at least annually to validate response procedures, communication protocols, and overall readiness.

Maintenance, Exercises, and Validation

Kyndryl's Enterprise Business Continuity program requires Business Continuity Plans to be regularly reviewed, maintained, and exercised to validate their effectiveness and support continual improvement. Business Areas are responsible for maintaining their Business Continuity Plans and conducting exercise and validation activities at least annually, as well as following significant organizational, operational, or technology changes.

The Enterprise Business Continuity Management (EBCM) function provides guidance, enablement, and awareness resources to support business continuity preparedness across the organization. Educational materials, tools, and resources are made available to employees and designated continuity stakeholders to strengthen resilience capabilities and promote consistent adoption of BCMS requirements.

Lessons learned from exercises and actual disruptive events are incorporated into continuity plans, recovery strategies, and program improvements to enhance response effectiveness and recovery readiness.

Frequently Asked Questions (FAQs)

General Business Resiliency

Does Kyndryl have a Business Continuity program?

Yes. Kyndryl maintains an established Enterprise Business Continuity Management (BCM) program that provides the strategy, governance framework, standards, and oversight necessary to support organizational resilience across the company.

The program adopts a risk- and impact-based approach to continuity management and includes policies, standards, procedures, and governance mechanisms that guide the identification of critical business processes, development and maintenance of Business Continuity Plans (BCPs), exercising and validation activities, and continuous improvement initiatives. The program is designed to strengthen Kyndryl's ability to anticipate, withstand, respond to, and recover from disruptive events while maintaining critical business operations.

What's Kyndryl's Business Continuity strategy?

Kyndryl's Business Continuity strategy is led by the Enterprise Business Continuity Management (EBCM) function and supported by business and technical stakeholders across the organization.

The strategy focuses on enhancing enterprise resilience through the identification and prioritization of critical business processes, supporting applications, infrastructure, personnel, facilities, and third-party dependencies. This is achieved through Business Impact Analyses (BIAs), risk assessments, and the implementation of appropriate continuity and recovery strategies.

Business Areas are accountable for maintaining and exercising Business Continuity Plans for critical processes within their respective areas of responsibility. These plans are reviewed, updated, and exercised on a regular basis, with annual exercise and validation activities conducted to support ongoing readiness, resilience, and continuous improvement.

Does Kyndryl have a formal governance body for Business Continuity?

Yes. Kyndryl has a formal governance structure led by the Enterprise Business Continuity Management (EBCM) function, which establishes enterprise-wide BCM standards, methodologies, and oversight. EBCM collaborates with business and technical stakeholders, including Enterprise Risk Management (ERM), Crisis Management teams, and the Chief Information Officer (CIO) organization, to promote a coordinated and integrated approach to resilience management across the enterprise.

Business Continuity is integrated into Kyndryl's Enterprise Risk Management (ERM) framework, ensuring that continuity-related risks are identified, assessed, monitored, and managed in alignment with enterprise risk management requirements.

Does Kyndryl have a team focused on Business Continuity and Disaster Recovery?

Yes. Kyndryl maintains a dedicated **Enterprise Business Continuity Management (EBCM)** function that provides governance, oversight, guidance, and enablement for the enterprise-wide Business Continuity Management System (BCMS). The EBCM function partners with Kyndryl Business Areas to strengthen continuity preparedness and resilience while supporting the delivery, modernization, and operation of mission-critical services and workloads.

The EBCM function establishes a consistent business continuity framework, standards, methodologies, and practices across the organization. It works closely with Business Areas through a global Business Continuity Guild and collaborates with stakeholders across Business Continuity, Disaster Recovery, Risk Management, Cybersecurity, Network Security, Incident Management, and Crisis Management to enhance organizational resilience.

In addition, Kyndryl leverages the expertise of **Kyndryl Security and Resiliency Services**, a globally recognized Business Continuity, Disaster Recovery, Cyber Resilience, and Recovery Services leader, which provides advisory, consulting, and managed resilience services that help customers strengthen continuity capabilities, recover from disruptions, and improve operational resilience.

Additional information regarding **Managed Continuity and Recovery Services, Disaster Recovery as a Service (DRaaS), and Cyber Resilience Services** is available through Kyndryl Security and Resiliency Services.
https://www.kyndryl.com/us/en/services/cyber-resilience

Has Kyndryl gained ISO 22301 certification or is there a timeframe for achieving it?

Kyndryl maintains a Business Continuity Management System (BCMS) that is aligned with ISO 22301, providing a structured framework for business continuity governance, risk assessment, continuity planning, exercising, maintenance, and continual improvement. While Kyndryl does not currently maintain a single enterprise-wide ISO 22301 certification, several Kyndryl locations and operations across various regions have achieved ISO 22301 certification based on local business, customer, and regulatory requirements.

Kyndryl continually evaluates its resilience capabilities and business continuity practices to ensure alignment with evolving customer, regulatory, and operational needs.

Information regarding Kyndryl certifications and compliance programs, including ISO certifications and other regulatory frameworks (such as ITAR, PCI DSS, and HIPAA), as well as details on specific Kyndryl entities, locations, or countries that hold ISO 22301 certification, can be provided upon request through a Kyndryl account representative.
https://www.kyndryl.com/in/en/compliance/certifications

How does Kyndryl evaluate Business Continuity risk?

Kyndryl evaluates Business Continuity risk through the assessment of critical business processes, supporting dependencies, recovery requirements, and potential disruption scenarios that could affect the organization's ability to deliver services. Assessments consider factors such as the criticality of business activities, geographic footprint, operational model, technology dependencies, workforce considerations, third-party dependencies, and regulatory obligations.

Senior management provides oversight of the enterprise risk and resilience framework, while business leaders are accountable for identifying, assessing, and managing Business Continuity risks within their areas of responsibility. Each business area is required to implement and maintain Business Continuity capabilities in accordance with Kyndryl's enterprise Business Continuity Management System (BCMS), policies, standards, and governance requirements.

How does Kyndryl conduct a business impact analysis?

Kyndryl conducts Business Impact Analyses (BIAs) to identify and prioritize critical business processes and evaluate the potential impacts of disruptions on business operations. The analysis documents and validates recovery requirements, including the Maximum Acceptable Outage (MAO), as defined by business process owners, and assesses critical dependencies such as personnel, facilities, technology, suppliers, third-party services, and process interdependencies.

Kyndryl takes a comprehensive approach to impact analysis by evaluating dependencies across business functions, geographic locations, and organizational boundaries. The BIA also considers end-to-end business processes and supply chain dependencies to develop an enterprise-wide understanding of critical operations and their interrelationships.

This approach enables Kyndryl to better understand the potential impacts of disruptions, identify continuity risks, and implement appropriate continuity and recovery strategies.

Business Continuity Plans

In the event of a disaster or significant disruption to critical business processes, does Kyndryl have documented plans for recovering critical business processes and IT?

Yes. Kyndryl's **Business Continuity Plans** are designed to restore essential business processes and functions, with priorities set based on business impact and risk assessments.

Additionally, **IT Disaster Recovery Plans**, which direct the restoration of IT services and applications supporting these critical processes, are prioritized by their business criticality. Kyndryl ensures that the critical services have documented plans in place and are regularly exercised to maintain readiness.

What type of scenarios or business interruptions does Kyndryl plan for?

Kyndryl prepares for various scenarios and business interruptions to support resilience and continuity. These include IT disruptions, workplace and workforce disruptions, cybersecurity incidents, regional and global events (Large-scale events that can affect multiple regions or the entire globe, such as geopolitical conflicts or widespread natural disasters), and supply chain disruptions. By planning for these scenarios, by preparing for these scenarios, Kyndryl aims to minimize downtime and ensure that critical business functions can continue operating smoothly.

In the event of a disaster or significant disruption, does Kyndryl have documented emergency plans?

Yes. Kyndryl maintains Emergency Management and Crisis Management capabilities designed to support preparedness for and response to disruptive events that may affect personnel, facilities, operations, or service delivery. At the enterprise level, Kyndryl's Corporate Crisis Management Team (CMT) provides strategic direction, coordination, governance, and policy guidance during significant events. Country and local Crisis Management Teams are responsible for executing response activities, safeguarding personnel, protecting company assets, minimizing operational impacts, and coordinating recovery efforts. These teams work closely with affected business areas to support continuity of operations and facilitate an effective response and recovery.

Has Kyndryl included any specific guidelines or measures for pandemic situations like COVID-19 in their Business Continuity Plans?

Yes. Kyndryl's Business Continuity Plans incorporate preparedness and response strategies for pandemic and other widespread health-related events. The plans consider scenarios that may affect workforce availability, access to facilities, supply chains, and the delivery of critical business services. They include recovery and continuity strategies intended to help sustain essential business operations and customer service delivery during such events.

Kyndryl continuously monitors emerging risks and public health developments through guidance issued by recognized authorities and trusted sources, including the World Health Organization (WHO) and relevant governmental agencies.

The Corporate Health and Safety organization, in collaboration with the Crisis Management Team (CMT) and Enterprise Business Continuity Management (EBCM) function, coordinates preparedness, response, and recovery activities related to pandemic events. Drawing on extensive experience in pandemic planning and response, Kyndryl maintains established processes and response strategies to address a broad range of health-related emergencies and operational disruptions.

What is Kyndryl's process for reviewing and signing off on Business Continuity Plans?

Kyndryl's Business Continuity Plans undergo review and approval by the relevant line management of the respective business areas where the plans are implemented.

How often does Kyndryl update or review their Business Continuity Plans?

Kyndryl reviews and updates its Business Continuity Plans at least annually as part of its established governance and maintenance processes. Plans are also reviewed and updated whenever significant changes occur to business operations, organizational structures, technologies, facilities, or other factors that could affect continuity and recovery capabilities, ensuring that plans remain current, effective, and aligned with business requirements.

Will Kyndryl provide customers with copies of their current Business Continuity Plans?

Kyndryl does not typically share Business Continuity Plans with customers due to the confidential and proprietary nature of these documents. However, Kyndryl provides customers with information regarding its Business Continuity Management Program, including its governance framework, recovery strategies, exercise and validation activities, and resilience capabilities, to help demonstrate preparedness for responding to and recovering from disruptive events. Additional information may be provided through customer due diligence, contractual mechanisms, or other agreed-upon assurance processes, as appropriate.

In the event of a disaster, does Kyndryl have Business Continuity Plans for services and solutions provided to customers that meet business recovery requirements?

Kyndryl maintains Business Continuity Plans and supporting recovery procedures to sustain and recover critical business operations that support the delivery of services to customers. These plans are designed to address a range of disruption scenarios, including technology outages, natural disasters, workforce disruptions, and other significant events.

Kyndryl's Business Continuity program supports the resilience of its global operations; however, customer-specific business continuity and recovery requirements may vary based on the services provided, contractual obligations, and solution design. Customers should engage directly with their Kyndryl account representative to discuss account-specific continuity and recovery requirements and to determine appropriate recovery strategies, mitigation measures, and service-level commitments.

Kyndryl's internal Business Continuity Plans complement, but do not replace, customer contractual agreements, service commitments, or customer-owned business continuity and disaster recovery plans.

How are customers notified if a disaster at Kyndryl affects their contracted services?

In the event of a disruption that materially affects contracted services, Kyndryl follows established incident management and communication processes to keep impacted customers informed. Communications may be coordinated through designated account representatives, service delivery teams, or other agreed communication channels, as appropriate to the nature and severity of the event.

Customers are provided with timely updates regarding the disruption, the potential impact on services, actions being taken to mitigate the issue, and progress toward service restoration. Communication frequency and escalation procedures may vary based on contractual obligations, service agreements, and the specific circumstances of the event.

Training, Exercising, and Maintenance

What is Kyndryl's approach to Business Continuity exercising and validation?

Kyndryl promotes organizational readiness through a structured Business Continuity training, awareness, and exercise program. The Enterprise Business Continuity Management (EBCM) team provides training and awareness resources for key personnel and makes educational materials available to employees globally.

Training requirements are established for relevant personnel to promote a consistent understanding of Business Continuity roles, responsibilities, and recovery procedures across the organization.

Kyndryl's approach to Business Continuity exercises and validation activities is designed to assess organizational preparedness and resilience across a range of disruption scenarios, including natural disasters, technology outages, workforce disruptions, and cybersecurity incidents.

The program includes:

Exercises and Validation Activities: Utilizing methods such as tabletop exercises, structured walkthroughs, simulations, and recovery validation activities to assess the effectiveness of continuity and recovery capabilities.

Continuous Improvement: Reviewing exercise results and lessons learned to identify improvement opportunities and enhance resilience.

Comprehensive Coverage: Evaluating critical business processes, technology, personnel, facilities, and key dependencies as part of continuity preparedness activities.

Business Continuity Plans are exercised periodically by the responsible business areas as part of the plan maintenance lifecycle. Following each exercise, observations and findings are reviewed, and improvement actions are tracked to completion to address identified gaps and strengthen preparedness.

Through ongoing exercising, validation, and review, Kyndryl continuously enhances its Business Continuity capabilities to maintain operational readiness and organizational resilience

Do internal or external auditors review Kyndryl's Business Continuity exercises and validation activities?

Yes. The results of Business Continuity exercises and validation activities may be reviewed by internal and external auditors as part of audit, compliance, or assurance reviews, depending on applicable contractual, regulatory, and business requirements

How often does Kyndryl exercise the Business Continuity Plans?

Kyndryl exercises and reviews Business Continuity Plans on a regular basis to support ongoing readiness and resilience. At a minimum, business areas conduct annual exercise and validation activities and update plans as necessary following significant organizational, operational, technology, or regulatory changes.

Kyndryl may conduct additional Business Continuity exercises and validation activities in response to significant business, operational, regulatory, or technology changes, as well as following actual incidents, to support the continual improvement of its Business Continuity Plans.

Will Kyndryl share Business Continuity Plan exercise results or conduct joint exercises with customers?

Kyndryl maintains strict confidentiality regarding the results of its Business Continuity exercises and validation activities and does not disclose such information to external parties unless required by contractual obligations or applicable legal and regulatory requirements. Customer-specific continuity and recovery requirements should be addressed directly with the appropriate Kyndryl account team.

How does Kyndryl understand proximity and impact on Kyndryl sites, Data centers, and employees located in a disaster area?

Kyndryl utilizes disaster monitoring and assessment platforms leveraging artificial intelligence, machine learning, and analytics to assess potential impacts to Kyndryl offices, data centers, and employee locations.

These platforms integrate information from multiple trusted sources, including government agencies, emergency management organizations, weather services, seismic monitoring agencies, and global news feeds, to identify and assess emerging threats and disruptive events. This capability supports situational awareness and enables timely evaluation of potential impacts on Kyndryl operations, facilities, technology assets, and personnel.

How frequently are Business Continuity Plans (BCPs) reviewed and updated at Kyndryl, and how does the EBCM team ensure compliance and continuous improvement through performance monitoring?

Plan Maintenance and Review: Business Continuity Plans are reviewed and updated at least annually and following significant organizational, operational, technology, regulatory, or risk-related changes. Business areas are responsible for maintaining, exercising, and validating their plans in accordance with established Business Continuity Management requirements.

The EBCM team monitors program performance through governance oversight, risk and performance indicators, exercise outcomes, and compliance assessments. Results from exercise and validation activities are documented and reviewed to identify improvement opportunities, track remediation activities, and support the continual enhancement of Kyndryl's Business Continuity Management program.

What kind of training and awareness efforts are in place for employees?

Kyndryl promotes Business Continuity awareness and preparedness through a comprehensive training, awareness, and exercise program. Training and educational resources are provided to employees globally to support an understanding of Business Continuity principles, roles, responsibilities, and recovery procedures.

Key elements of Kyndryl's approach include:

- **Role-Based Training:** Business Continuity personnel and key stakeholders receive training appropriate to their Business Continuity responsibilities.
- **Awareness and Education:** Business Continuity awareness materials are made available through internal communications, collaboration platforms, and educational resources.

- **Knowledge Sharing and Best Practices:** The Enterprise Business Continuity Management (EBCM) team fosters a global community that promotes the sharing of expertise, lessons learned, and industry best practices across Kyndryl.
- **Business Continuity Awareness Week:** Kyndryl conducts awareness initiatives and educational events to strengthen employee understanding of resilience, preparedness, and continuity practices.
- **Exercises and Validation Activities:** Personnel participate in periodic exercises and validation activities, including tabletop exercises, walkthroughs, and scenario-based activities, to enhance preparedness and validate continuity capabilities.
- **Continuous Improvement:** Feedback, lessons learned, and exercise outcomes are used to continuously improve Business Continuity Plans, training programs, and overall organizational resilience

Recovery Strategy

Does Kyndryl have specific workplace recovery locations for critical sites?

Yes. Kyndryl maintains recovery strategies designed to support the continuity of critical business operations in the event that a primary work location becomes unavailable. Given Kyndryl's global operating model and presence across multiple countries, recovery strategies leverage geographically dispersed locations, flexible workforce arrangements, and alternative work capabilities rather than reliance on a single recovery site.

When developing workplace recovery strategies, Kyndryl considers factors such as geographic diversity, accessibility, workforce availability, infrastructure capabilities, operational requirements, security considerations, and applicable regulatory obligations to support business continuity and operational resilience.

Does Kyndryl's Business Continuity Plans cover sites that deliver services and solutions to customers?

Yes. Kyndryl's Business Continuity Program encompasses critical business processes and supporting operations, including functions that support the delivery of services and solutions to customers. Continuity strategies leverage Kyndryl's global operating model, geographically distributed teams, diverse workforce, and operational flexibility to support the ongoing delivery of services during disruptive events.

Where applicable, continuity and recovery considerations are incorporated into operational processes to help mitigate the impact of site-specific disruptions. Customer-specific continuity and recovery requirements may vary based on contractual commitments, service design, and the nature of the services provided.

Third-party Suppliers

Kyndryl has implemented a comprehensive third-party risk management (TPRM) platform that enables us to proactively identify, assess, and mitigate risks across our entire supplier and partner ecosystems.

We use the platform for continuous monitoring and automated risk scoring, helping procurement and compliance teams move from periodic due diligence to real-time risk oversight.

By integrating risk insights directly into our sourcing process and supplier management workflows, we drive informed decision-making while strengthening regulatory compliance and protecting our brand reputation.

Does Kyndryl assess the Business Continuity preparedness of their strategic suppliers?

Yes, Kyndryl assesses the Business Continuity preparedness of its strategic and critical suppliers as part of its supplier risk management framework.

Kyndryl's Global Procurement organization operates a Supplier Business Continuity Assessment Program designed to evaluate supplier resilience and readiness to support the continuity of Kyndryl services, solutions, internal operations, and customer obligations. The assessment reviews a supplier's ability to establish, maintain, and periodically exercise appropriate Business Continuity and recovery capabilities, helping ensure they can continue supporting critical products and services during disruptive events.

What does the Kyndryl Supplier Risk Management program cover?

Kyndryl's Supplier Risk Management program addresses a broad range of risks that could impact a supplier's ability to meet contractual obligations and support business continuity requirements. Areas assessed include, but are not limited to:

- **Financial viability and stability**
- **Information security and cybersecurity controls**
- **Business continuity and resilience capabilities**
- **Social, environmental, and ESG considerations**
- **Regulatory and compliance requirements**
- **Import/Export regulations and trade compliance**
- **Anti-corruption and ethical business conduct requirements**
- **Operational, geographic, and concentration risks**

This risk-based approach helps Kyndryl identify potential vulnerabilities across the supply chain and implement appropriate mitigation, monitoring, and response measures to minimize disruption to Kyndryl operations and customer services.

kyndryl

© Copyright Kyndryl, Inc. 2026

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.