Always ensuring business continuity

Infobip's Business Continuity Program White paper

In today's digital-first world, staying in touch with your customers is imperative. At Infobip, we are committed to helping our clients, partners, and end-customers stay connected, always.

Our leading omnichannel communications platform powers 495+ billion interactions annually with flexible APIs, CPaaS capabilities, security and authentication solutions, and SaaS solutions built on a resilient infrastructure to facilitate a superior customer experience while mitigating risks associated with on-demand global communications at scale.

Our Business Continuity Management Program with our robust plans and capabilities ensure continuous delivery of high quality technical and business services.

Resilience, availability, reliability, and security of our platform and products as well as people supporting these activities are crucial for our clients and partners to build connections and trust with their customers.

We ensure the above, by building practices for operational and development processes, our robust and reliable platform, and our Business Continuity Management Program.

/* Key takeaways

The Infobip Business Continuity Program ensures always-on delivery of our most important products and solutions during any disruption.

We prioritize:

- **People:** our most valuable assets
- **Products and solutions:** our building blocks for continuous interactions
- **Clients, partners, and end-customers:** our customer experience eco-system
- **Security, integrity, and availability of data:** our source for insights and knowledge

---

To further demonstrate our commitment to increasing our resilience and continuous improvement of business continuity and ability to safeguard critical operation **Infobip has completed ISO 22301 certification.**

The certificate is available for download from our website.

We know how vital continuous communication is to business success. To ensure you never have to worry, we have set out a Business Continuity Management Program. Read this white paper to gain further insights into:

- // Our Program
- // Our response structure
- // Why is this important
- // Our commitment
- // Our certifications

// Our Program

Infobip follows the ISO 22301 definition on business continuity:

> The capability of the business to continue the delivery of products and services at acceptable, predefined levels following a business disruption.

In a nutshell, we aim to provide our employees, partners, clients, and their end-customers with the assurance in our ability to provide reliable products and solutions for continuous communication. The key principles of our Business Continuity Program are:

Prioritizing uninterrupted provision of our most important products and services

Ensuring internal processes and teams can support delivery of products and services during unforeseen circumstances and events

Continuous improvement of our Business Continuity Program and development strategies

The scope of our Business Continuity Program covers prioritized customer-facing products and solutions, internal processes and teams supporting their delivery.

Our program is certified against ISO 22301 Business Continuity Management System and is also aligned with Business Continuity Institutes' Good Practice Guidelines.

The team behind our program

We have a dedicated Business Continuity Management team within our Corporate Security Department. This team is comprised of our leaders and industry certified experts who have extensive experience in designing and implementing business continuity strategies, along with expertise in regulatory frameworks, compliance, and cloud communications. The team is strategically positioned in a cross-functional department to enable collaboration and facilitate successful mitigation of risks, crisis planning and implementation of the Program.

Our approach

Based on our business objectives, in line with the company's strategic goals, and prioritizing the needs of our clients and partners, the Business Continuity Management Team has worked on a robust approach to ensure continuity of services.

The implementation of our Business Continuity Program started by establishing policy and framework, objectives, and scope of Program. The scope of the Program has been determined by Business Impact Analysis (BIA), Risk Assessment (RA) and in line with related legal and regulatory requirements. This has been undertaken to determine the prioritized services and the resources needed to maintain delivery that meets the standards our customers and partners expect of us. The RA process identifies and assesses the risks to these critical assets to support efficient and effective, focused planning of our efforts.

As an engineering powerhouse we understand the importance of a secure, reliable, and robust platform, and the need to always provide a high level of service quality that our clients and partners expect.

Objectives behind our Business Continuity Program

Protection	Risk reduction	Assurance	Compliance
Our Program ensures our people, or Bippers as we fondly call ourselves, have a secure and healthy working environment. This in turn safeguards the service provided to our clients and partners.	Our Program regularly assesses and continuously tracks any potential risks or threat. This helps us proactively mitigate threats and take a holistic approach in providing an always-on delivery of services and products.	Our Program lays out the steps required to provide uninterrupted services even during the most challenging times. Our customers and partners can trust that we are always available and reliable.	Our Program is aligned to the international Business Continuity Management Systems standard and best practices. In addition, our global expertise and local footprints ensures we are compliant in all markets where we maintain presence.

As results of business impact analysis and risk assessment, response and recovery strategies are developed and response structure defined. Based on possible strategies, solutions are selected and implemented in plans and procedures. Read further to gain insights on how the response structure is established and what plans are essential.

// Our response structure

Our business continuity response structure is a robust framework designed to ensure seamless operations during disruptions. It comprises of dedicated teams responsible for various aspects of continuity, including crisis management, resource allocation, and communication.

Our Business Continuity Response structure is divided into the following response levels:

- **Strategic response**
- **Tactical response**
- **Operational response**

This structure ensures efficient coordination, decision-making, and communication, enabling a timely and effective response to mitigate risks, minimize operational disruptions, protect employees and assets, and maintain transparency and customer trust. Regular testing, training, and updates ensure the efficacy of the response structure and plans, enabling us to navigate challenges and maintain operational resilience.

Strategic Response

Strategic response involves high-level decision-making, policy development, and resource allocation for organizational resilience.

The Business Continuity Policy is the key document that sets out intentions and direction of Infobip, as formally expressed, by our top management, while Business Continuity Strategies identify the possible options to continue providing services and selection of most appropriate solutions.

Crisis Management Plan

Our Crisis Management Plan provides guidelines, tools and decision criterias to assist in expediting the key phases of Crisis Management. It includes a clear chain of command, communication protocols, and designated roles and responsibilities for key individuals.

Crisis Communication Plan provides various communication formats dependent on the incident and designates specific individuals as the only authority for answering questions or communicate all information both internally and externally to all interested parties.

The strategical team or Crisis Management Team is responsible for any crisis affecting the whole organization. Members of the crisis team consist of top management with global responsibilities and experienced managers with the authority to apply the organization’s complete resources to respond.

Tactical response

Tactical response focuses on incident response planning, resource management, training, and communication. The tactical team or Business Continuity Management Team manages and coordinates the activities needed to deliver the impacted products, services, and recovery of office location functions.

Our Business Continuity Incident Response Plan describes the process for assessing the situation, assembling recovery teams, activating plans, and making critical decisions. The protocols developed as part of this plan include triggers for activation and escalation criteria based on the severity of an incident.

Business Continuity Plan for offices

Infobip leverages its comprehensive communications platform to swiftly respond to environmental and man-made disasters and ensure the safety of its employees and office locations. The platform's robust features enable us to assess the impact of disaster on affected facilities, coordinate rescue and relief efforts, and maintain continuous communication to ensure the well-being of our employees and the operational integrity of our offices.

At Infobip, we are setup for exponential growth while maintaining resilience. Our products and services are fully operational globally, with support in 70+ offices across six continents. Assuring confidence in our ability to deliver the highest levels of performance, availability, and security.

Additionally, we have 40+ data centers across the world, ensuring our communications platform runs reliably and our customers and partners benefit from our ability to scale, or re-provision infrastructure resources as required across multiple locations, using the same tools, APIs, partners, and solutions. This includes computing resources, storage and database resources, networking, security, and DNS.

Our response and recovery mechanisms are tested and updated regularly to ensure the security, reliability, and availability of our products and services.

Disaster Recovery Plans

Our communications platform is built with resilience by design. Response and recovery strategies have been developed to mitigate the impact on critical services during a disruptive incident. Recovery Time Objectives (RTOs) are set based on possible impacts from a disruption. These plans are developed, managed, reviewed, monitored, and tested by the Business Continuity Management team and Business Continuity and Disaster Recovery Group.

Our disaster recovery solution begins with:

- Building robust and resilient infrastructure in each of our data center locations
- Developing and managing our very own platform
- Following best practices and industry standards

Our plans are structured to enable the recovery of our products and services as soon as possible. We evaluate the business continuity capabilities of key vendors and third parties that are supporting prioritized services and products through a supplier assessment process managed by the Corporate Security team.

Our Recovery Point Objectives ensure sufficient timeframes to enable us to meet our SLAs, obligations, and increase customer satisfaction.

This is achieved through procedures that define backup frequencies for relevant data in line with acceptable data loss parameters. Backup copies are protected with appropriate control mechanisms and recovery testing is periodically conducted to validate the integrity of backed-up information and to verify the duration of the recovery process.

Operational Response and Incident Management

Operational response encompasses activating various incident management teams and performing recovery actions. The operational teams or Incident Management Teams deal with the immediate effects of an incident, managing direct consequences and executing activities after the occurrence of an unplanned event.

Emergency Response Guidelines describes how to initially respond to a disruption related to natural disasters, unprecedented situations and threats that have potential to negatively affect the health, safety, and welfare of Infobip employees and/or the integrity of our buildings or environment, which is not covered by routine, day-to-day operations.

Cyber incident response

The cyber incident response process establishes playbooks to address cyber-attacks against our information systems. These playbooks are designed to enable security personnel to identify, mitigate, and recover from malicious cyber incidents, such as unauthorized access to a system or data, denial of service, or unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data.

Availability Incident Response Teams observe and respond to any events that might affect quality of our services delivery or internal tools. The Infobip Incident Status page https://status.infobip.com/ displays ongoing and past platform incidents impacting our products or services and upcoming maintenances that could affect service performance.

The people, processes, and technology necessary to conduct our business are distributed among our sites, with critical business operations conducted at multiple globally diverse locations. The process and protocol are in place to ensure guaranteed service levels to our clients.

// Why is this important

At a time when downtime is unacceptable, business continuity is critical. Our Business Continuity Program considers the risks and threats that could have a major or severe impact on our operational capabilities even if the probability of such events is very low. To prepare for these rare situations response and recovery plans are created and tested.

Why is it important for our partners and clients

Peace of mind with contingency plans when disaster strikes

Recover and resume in a pre-defined period of time

Assurance and confidence in service delivery

Continuous business ensuring minimal revenue impact

Resilient platform saving time, money, and reputation

// Our commitment

We are committed to provide products, solutions and services during any circumstance which is fortified by our business continuity plans and arrangements.

Business Continuity plans and arrangements are reviewed and exercised annually using a variety of scenarios and exercise types to ensure plans and procedures remain valid, efficient, effective, and consistent with our objectives.

Training and awareness plans are developed to enhance the competency and awareness of our people with valuable training, support, and development exercises. The Business Continuity Management Program is promoted across the organization at all levels through education to facilitate its successful embedding into normal business processes.

Business Continuity Management performance indicators have been developed to help monitor and measure the performance against the requirements set out in Policy and Program.

Our management annually performs a review of the Program and processes along with inspections from our Internal Audit department in line with their annual audit plans. Self-assessment, an assessment of the Program by the entire Business Continuity team are conducted annually as well. The reviewed actions are monitored to support continuous improvement.

We demonstrate continuous improvement of our Program by ensuring observations and non-conformities identified are progressed to resolution and, where appropriate, reflected in arrangements during reviews.

// Our certifications

Infobip's commitment to ensuring the highest possible quality and security of services provided to clients, and of our systems is evidenced through continuous investments in improvement of our controls. This is achieved through multiple certifications and compliance being regularly assessed internally and/or externally by renowned independent third parties.

ISO 22301 certification provides clients with the assurance that Infobip has a robust business continuity management system in place, emphasize our commitment to resilience, risk management, and continuity of critical operations. It helps foster trust and confidence in our ability to deliver products or services consistently, even in the face of disruptions with full transparency toward our stakeholders.

ISO 22301 is a standard developed by the International Organization for Standardization (ISO) that provides a framework for establishing, implementing, maintaining, and continually improving Business Continuity Management System (BCMS). The standard focuses on ensuring organizations can effectively respond to and recover from disruptive incidents while maintain critical business functions during times of crisis.

Infobip's other ISO certificates:

ISO 27001	ISO 9001	ISO 27017	ISO 27018

Infobip is GSMA open Connectivity, Cyber essential certificated and HIPPA, SOC 2 Type 2 and CSA STAR Level 1 compliant, among others. Compliance with standards and frameworks is assessed on an annual basis and certificates are available for download from our web page: https://www.infobip.com/certificates

Infobip's Business Continuity Program is a critical component in maintaining the high standard of service we have established as we continue to grow and expand our platform and product pallet. Resilience and reliability are a continual effort and our investment in the business continuity program reflects our commitment to protecting our people, clients, and products.