GupShup Technology India Private Limited

SOC 2® – System and Organization Controls for Service Organizations: Trust Services Criteria

Description of GupShup Technology India Private Limited's Conversational Messaging Platform and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality

With the Report of Independent Service Auditor

As of September 30, 2022

Table of Contents

Gupshup Technology India Private Limited's Management Assertion

October 28, 2022

We have prepared the accompanying ” Description of Gupshup Technology India Private Limited's Conversational Messaging and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality” (Description) of Gupshup Technology India Private Limited (Gupshup) (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the “Description of Gupshup Technology India Private Limited's Conversational Messaging and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality” (System) that may be useful when assessing the risks from interactions with the System as of September 30, 2022, particularly information about system controls that Gupshup has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

GupShup uses Amazon Web Services (AWS) – a third-party cloud service provider, NTT Netmagic – a third-party colocation data center and Freshworks – a unified customer service platform in relation its Conversational Messaging Platform and Bot Development Services. The Description includes only the controls of GupShup and excludes controls of AWS, NTT Netmagic and Freshworks. The Description also indicates that certain trust services criteria specified therein can be met only if AWS's, NTT Netmagic's and Freshworks' controls assumed in the design of GupShup's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to the controls of AWS, NTT Netmagic and Freshworks.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Gupshup's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

a. The Description presents the System that was designed and implemented as of September 30, 2022, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed and implemented to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Gupshup’s controls as of September 30, 2022.

Signature:

Nilesh
Shivaji
Sonawane

Digitally signed by
Nilesh Shivaji
Sonawane
Date: 2022.10.28
13:20:19 +05'30'

Name: Nilesh Sonawane

Designation: Senior Director – Finance Controller

Ernst and Young Associates LLP
12th & 13th Floor
"UB City" Canberra Block
No. 24, Vittal Mallya Road
Bengaluru – 560001, India

Tel: +91 80 6727 5000
Fax: +91 80 2201 6000

ey.com

Independent Service Auditor's Report

To: GupShup Technology India Private Limited

Scope

We have examined GupShup Technology India Private Limited's (GupShup) accompanying "*Description of GupShup Technology India Private Limited's Conversational Messaging Platform and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality*" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design of controls included in the Description as of 30 September 2022 to provide reasonable assurance that GupShup's service commitments and system requirements would be achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

GupShup uses Amazon Web Services (AWS) – a third-party cloud service provider, NTT Netmagic – a third-party colocation data center and Freshworks – a unified customer service platform in relation its Conversational Messaging Platform and Bot Development Services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GupShup, to achieve GupShup's service commitments and system requirements based on the applicable trust services criteria. The description presents GupShup's system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been suitably designed and implemented at Amazon Web Services, NTT Netmagic and Freshworks. Our examination did not extend to the services provided by Amazon Web Services, NTT Netmagic and Freshworks, and we have not evaluated whether the controls management assumes have been implemented at Amazon Web Services, NTT Netmagic and Freshworks or whether such controls were suitably designed and implemented as of 30 September 2022.

The Description also indicates that GupShup's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of GupShup's controls are suitably designed and implemented, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design of such complementary user entity controls.

GupShup's responsibilities

GupShup is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. GupShup has provided the accompanying assertion titled, "*GupShup Technology India Private Limited's Management Assertion*" (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if operating effectively. GupShup is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design of the controls described therein to achieve the Service Organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, if operating effectively, based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria

- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if the controls operated effectively
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed based on the applicable trust services criteria
- evaluating the overall presentation of the Description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent of GupShup and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement.

Inherent limitations
The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own needs.

Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the Description, or conclusions about the suitability of the design of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Other matter
We did not perform any procedures regarding the operating effectiveness of controls stated in the description, and, accordingly, do not express an opinion thereon.

Opinion
In our opinion, in all material respects:

a. the Description presents the "*Description of GupShup Technology India Private Limited's Conversational Messaging Platform and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confident*iality" (Description) system that was designed and implemented as of 30 September 2022 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed as of 30 September 2022, to provide reasonable assurance that GupShup’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date.

Restricted use

This report is intended solely for the information and use of GupShup, user entities of GupShup’s as of 30 September 2022, prospective user entities, independent auditors, and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization’s system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization’s controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

For Ernst & Young Associates LLP

Anuj Gupta
Partner
28 October 2022

Description of GupShup Technology India Private Limited's Conversational Messaging Platform and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality

Overview of Operations

GupShup Technology India Private Limited (GupShup) is a provider of conversational messaging APIs for companies across the globe. GupShup solutions are designed to enable customers to engage with their end users through conversational experiences. GupShup's carrier-grade platform provides a single messaging API for Various messaging channels like WhatsApp, Messenger, Instagram etc. GupShup offers APIs for developers to build interactive, programmable, and omni-channel messaging services to enable in-app messaging. GupShup is headquartered in San Francisco, California, USA. GupShup is ISO 27001:2013 certified.

GupShup Service Delivery Models

GupShup services are bifurcated into:

- Enterprise
- Self-serve

Enterprise model involves providing customized solutions to large clients through service contracts. Self-serve model is offered to Small and Medium Enterprises (SME)/individual end users through the GupShup.io website.

GupShup Products

GupShup predominantly provides SMS, IP messaging, and chatbot services to banking, financial services, and insurance (BFSI), retail, and e-commerce companies. GupShup also offers value added services such as Bot development and Bot hosting, agent dashboards, e-commerce integration and custom APIs. GupShup's solutions and services encompasses the following:

- Conversational Messaging API
- GupShup Payment App
- Feature phone payments through secure messaging
- WhatsApp Customer Support
- Appointment booking
- Marketing Dashboard
- Food & Beverage
- Retail
- 1-Click Bill Pay
- Agent Dashboard

Principal Service Commitments and System Requirements

GupShup designs its processes and procedures to meet its objectives for the "Description of GupShup Technology India Private Limited's Conversational Messaging Platform and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality" (System). Those objectives are based on the service commitments that GupShup makes to user entities (customers) and requirements that GupShup has established for the services. GupShup is responsible for its service commitments and system requirements and for designing and implementing controls within the system to provide reasonable assurance that GupShup's service commitments and system requirements are achieved.

Security, Availability and Confidentiality commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the GupShup. Security, Availability and Confidentiality commitments are standardized and include, but are not limited to, the following:

- GupShup's objectives are based on the applicable laws, regulations, compliance requirements, and service commitments made to clients that GupShup has established for its services.
- Services include conversational messaging services through various channels such as SMS, WhatsApp, Facebook, etc. GupShup also provides services such as Bot development and Bot hosting, agent dashboards, e-commerce integration and custom APIs.
- GupShup establishes security and availability commitments to user entities pertaining to the service commitments. GupShup also establishes operational requirements that support the achievement of security and availability commitments, compliance of relevant laws and regulations, and other system requirements.
- As it relates to security, availability, confidentiality, GupShup has defined Information Security Management System (ISMS) which includes policies and process around hiring, training, system design and development, implementation of appropriate administrative, technical, and physical safeguards and controls.
- System requirements in place to meet the security, availability, and confidentiality commitments of GupShup include, but are not limited to, the following:
    - Intrusion-detection systems to monitor unauthorized access attempts;
    - Automated tools to continuously monitor and log server availability;
    - Firewalls to protect systems and networks;
    - Encryption techniques to secure data storage and transmission;
    - Business continuity and disaster recovery plan to counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems or disasters.

Scope

The scope is intended to meet the criteria for the Security, Availability, and Confidentiality, categories set forth in *TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids) (Applicable Trust Services Criteria) for Description of GupShup Technology India Private Limited's Conversational Messaging Platform and Bot Development Services, relevant to Trust Services Criteria of Security, Availability, and Confidentiality related services provided to user entities, from the following Delivery Centers:

Location	Address
Bangalore, India	Eastland Citadel, #150/1, Ground Floor, Hosur Main Road, Kaveri Layout, S.G. Palya, Koramangala, Bengaluru, Karnataka, 560029, India
Chennai, India	Amarasri building, #455, 7th Floor, Anna Salai, Teynampet, Chennai, Tamil Nadu, 600018, India
Mumbai, India	101 Silver Metropolis, 1st Floor, Western Express Highway, Goregaon (E), Mumbai, Maharashtra, 400063, India

Gupshup offers the following products and services to its customers:

Conversational Messaging Platform:

Gupshup provides Conversational Messaging Platform for its clients to communicate SMS, Voice, Email, WhatsApp, and Bot based information to their customers with a single Application Programming Interface (API). This API helps user entities to interact with their customers through various messaging channels. The following solutions are offered via the Conversation Messaging API.

Solutions	Description
GupShup Payment App	This mobile application is currently available only on feature phones (Phones with basic multimedia capabilities but cannot connect to Internet) and enables end users to complete the payments securely to merchants by scanning the QR Code by integrating the camera access of their devices. The GupShup Payment App can also be used for receiving funds as the App generates a QR Code and displays it on the phone screen. Furthermore, the GupShup Payment App also has some "Value Added Features" such as transaction history, user configuration, pay again and retry payment.

Solutions	Description
Feature phone payments through secure messaging	This solution enables end users with feature phones to complete the bill payments securely to merchants through the contextual one-click payment option available on the "SMS" app. Alternately, payments can also be processed from the "Contacts" app.
WhatsApp Customer Support	This service helps clients to create a WhatsApp customer support tool on GupShup sandbox environment. This service empowers customer support teams to communicate with their potential end users instantly through this tool to address sales queries and troubleshooting issues.
Appointment Booking	This solution helps Small and Medium Enterprises (SME) customers for improving the appointment booking process through GupShup IP (an IP Messaging Channel provided by GupShup, that works on any device without any application), smart messaging and integrated calendar.
Marketing Dashboard	This solution enables both enterprise and self-serve customers for creating dynamic marketing campaigns for driving traffic and enhancing the brand awareness. GupShup customers can publish a campaign by adding contact lists either manually or by uploading a csv file containing the end user contact data. Personalized message templates can be created for the targeted end users. Campaigns can be published right away through WhatsApp and or SMS channels. Campaigns can also be saved and scheduled for a later date. Scheduled campaigns can be edited or deleted later as per the customer's requirements.
Food & Beverage	This solution provides a product catalogue manager that helps restaurants in creating, customizing, and managing a contactless digital menu. End users can scan the respective QR code, and the digital menu is hosted on GupShup IP (GIP) User Interface is displayed wherein the customers can place their orders and track the status.
Retail	This solution provides a product catalogue manager that helps merchants with creating, customizing, and managing their catalogue of products. Further, the merchant's customers can view and order products through the front-end.

Solutions	Description
1-Click Bill Pay	1- Click Bill Payment converts a normal message into an AI powered actionable payment reminder message. It enables customers to make direct bill payments from their messages through a single click payment link/button. GupShup AI inserts UPI deep links across Various messaging channels like WhatsApp, Messenger, Instagram etc. by fetching the payment information from the message content.
Agent Dashboard	Agent Dashboard is a solution to monitor and respond to all incoming/two-way messages on your social media channels such as WhatsApp Business number, Google Business Manager, Instagram Channel, GupShup Messaging channel (GIP) & more. It provides quick access to chats based on criteria that will help the agents to prioritize their work. The dashboard provides visibility to the vital conversation and productivity metrics to identify the gaps to remove shortcomings and improve performance and ultimately customer satisfaction

Bot Development Services:

This service provides customers a platform to develop bots to build intelligent chatbots and voice assistants. Bots can be custom developed as per the specific requirements of the customer and be deployed across Various messaging channels including WhatsApp, Telegram, Facebook Messenger etc.

The report includes the description and related controls of commonly executed processes by GupShup across all its user organizations and does not include description related to specific processes that are applicable only to certain user organizations. This report does not include any other services or locations of GupShup apart from what has been described in this report.

Subservice Organization

GupShup uses Amazon Web Services (AWS), a third-party cloud service provider and NTT Netmagic, a third-party datacenter provider for hosting the infrastructure in relation to the products and services provided.

This report does not include services provided by the subservice organizations. The controls related to Subservice Organizations' processes and procedures are excluded from the scope of the Description, using the carve-out Method of reporting.

Complementary User Entity Controls

In designing its system, GupShup has contemplated those certain complementary controls would be implemented by user entities to meet certain criteria applicable to security, availability, and confidentiality. The complementary user entity controls are listed in the section '*Description of Trust Service Criteria and Related Controls*' and summarized in Appendix A.

Complementary Subservice Organization Controls

In designing its system, GupShup has contemplated those certain complementary controls would be implemented by their third-party service providers to meet certain criteria applicable to security, availability, and confidentiality. The complementary subservice organization controls are listed in the section '*Description of Trust Service Criteria and Related Controls*' and summarized in Appendix B.

Relevant aspects of the Control Environment, Risk Assessment, Monitoring and Communication and Information

Control Environment

GupShup has established an internal controls framework that includes:

- The overall control environment within the organization and its various processes,
- Risk assessment procedures,
- Control activities that help in meeting the overall control objectives,
- The monitoring components of internal control, and
- Information and communication procedures.

The following is a description of the key components of GupShup's internal control environment:

Organizational Structure

The organizational structure of GupShup, which provides the overall framework for planning, directing, and controlling operations, has segregated personnel and business functions according to job responsibilities. GupShup operates under the general direction and supervision of its Board of Directors (BoD).

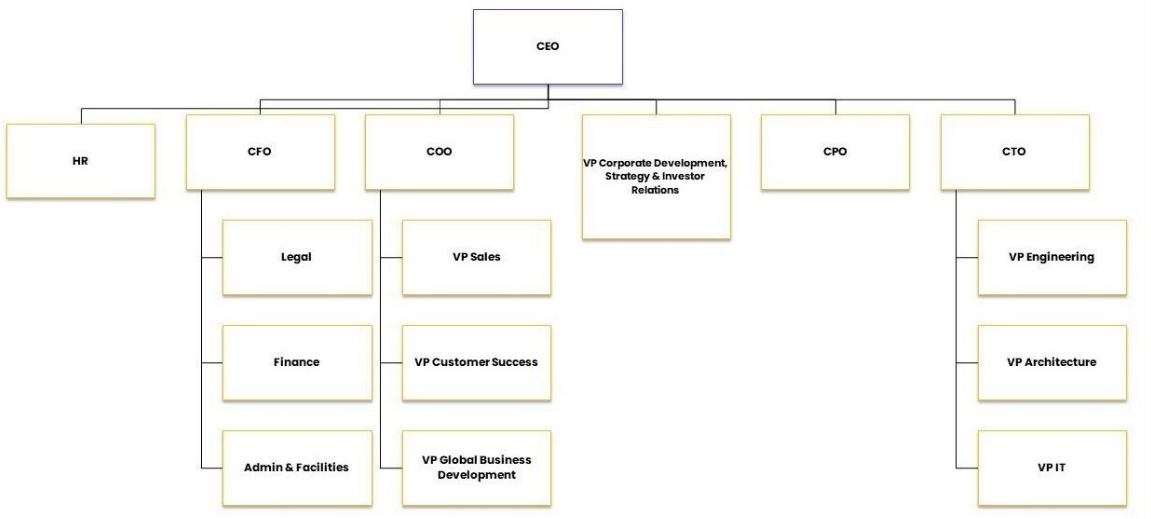

Figure 1: Organization Structure at GupShup

Governance Structure

Board of Directors (BoD)

The Board of Directors (BoD) consists of the Chief Financial Officer (CFO) and the Finance Controller of GupShup. The Board of Directors provides leadership and direction to the organization and is responsible for protecting the interests of the company and its major stakeholders, the employees, the customers, and the debt holders. The BoD is also responsible for selection, evaluation, development, and compensation of senior management. Additionally, the board of directors convene to discuss about the policy changes, annual financial statements, and findings of the Audit Committee Meetings on a quarterly basis.

Chief Executive Officer (CEO)

The CEO of GupShup is responsible for the following:

- Establishing and leading the Senior Executive team,
- Setting Direction and goals for the Organization,
- Establishing & institutionalization of the company culture and values,
- Provide direction for innovation and growth,
- Responsible for driving company's market share,
- Evaluate the effectiveness of security,
- Oversee a policy of process integration, and
- Provide leadership vision.

Chief Operating Officer (COO)

The COO of GupShup is responsible for:

- Overall health and growth of all Business Units, technology enablers, global Business Development, Customer Success and Sales aspects of the organization,
- Strategy development and execution,
- Global responsibility of delivery and customer satisfaction,
- Collaboration of all the vertical and horizontal business and functional units for business effectiveness, and
- Sponsoring key business initiatives.

Chief Financial Officer (CFO)

The CFO of GupShup is responsible for:

- Admin & Facilities, Finance, and legal aspects of the organization,
- Company's financial metrics,
- Capital and allocation of the same based on business priorities,
- Responsible for Mergers & Acquisitions,
- Responsible for protecting the interests of the company and its stakeholders,
- Evaluate the annual financial statements and policy changes,

- Drive strategy to meet organizational top line and bottom-line goals, and
- Provide leadership vision.

Chief Product Officer (CPO)

The CPO of GupShup is responsible to:

- Act as the primary stakeholder and the evangelist for our enterprise data & insights products and rally our teams to reach new heights
- Engage with internal and external stakeholders to align on product strategy and priorities that deliver measurable results
- Define and own the strategic vision and roadmap for our enterprise data & insights products and communicate it effectively and passionately across the company
- Create go-to-market strategies for new product offerings
- Work with Product Marketing to develop a clear and compelling Marketing Strategy for our products
- Partner with Sales & Client Delivery teams to deeply understand customer needs and reflect them in our product roadmap
- Build a strong external presence and be an external evangelist for our product vision, technology, and product roadmap, influencing our customers, industry analysts and key partners
- Further grow our product management & design teams and build a world-class product organization that product manager's relish being a part of. Scale our product teams by coaching and mentoring our current team members and inspiring them with a compelling vision & strategy and by recruiting additional top talent
- Define and own product OKRs & roadmap and conduct quarterly product reviews
- Drive product planning, product definition, tactical execution, user engagement and feedback cycles Partner with internal stakeholders including engineering & marketing teams to unlock product innovation.

Vice President (VP) for Corporate Development, Strategy & Investor Relation of GupShup

The VP Corporate Development, Strategy & Investor Relation of GupShup is responsible to:

- Develop research, analysis, and financial models to drive business case development for key strategic focus areas.
- Engage with Investors – manage existing and prospective relationships in coordination with the CFO and CEO.
- Drive the mergers and acquisitions process. Define M&A strategy, maintain pipeline, evaluate opportunities, lead diligence activities, and provide general transaction and analytical support.
- Develop the Business Case methodology – establish a standardized way for leadership to test new business initiatives that are candidate projects or programs including but not limited to: scorecard/benchmarking of initiatives, assessing project prioritization, and evaluating risk assessments.
- Plan, organize, and supervise the work related to any new initiative, assess

progress, analyze results obtained, and recommend adjustments as required to achieve the stated objectives of the opportunity.

- Support key strategic priorities and projects in partnership with the CEO and CFO and working with other functions and stakeholders as required.
- Responsible for overseeing the finance business case process, investment analysis, analytics, scorecard/benchmarking of initiatives, cash flow modeling, and evaluating return. This analysis is used to prioritize initiatives, evaluate resource needs based upon a strategic business assessment.
- Support key strategic priorities and projects in partnership with the CEO and CFO and working with other functions and stakeholders as required.
- Interface with investment bankers, brokers, and consultants for acquisition opportunities.

Chief Technical Officer (CTO)

The CTO of GupShup is responsible to:

- Set the company's strategic direction, development, and future growth.
- Develop the company's strategy for using technological resources.
- Ensure technologies are used efficiently, profitably, and securely
- Work closely with Product, Design and GTM leadership on strategic planning, product development and execution.
- Recruit, retain, and develop great engineers who form cohesive teams capable of learning and growing.
- Track, produce, analyze, and action upon key metrics & milestones to ensure quality products are delivered on time.
- Communicate and collaborate with clients, partners, and vendors on technical details.
- Establish and maintain a world class engineering culture dedicated to craft, quality and impact.
- Use strong organizational leadership skills, self-motivation, and growth-oriented mind-set to lead, motivate, and inspire multiple teams of engineers to deliver high-quality software and be held accountable for their performance.
- Develop, communicate, and implement strategy for achieving the GTO mission, vision, and values within the function.

Chief Information Security Officer (CISO)

The CISO of GupShup is responsible to:

- Execute the overall Enterprise vision of information security across the organization,
- Develop security strategy, oversee the security program and initiatives, and liaise with business process owners,
- Ensure that risk and business impact assessments are conducted on a timely basis,
- Monitor utilization and effectiveness of security resources,

- Develop, implement, and monitor information security activities,
- Develop risk mitigation strategies and oversee a policy of risk management,
- Enforce security policies and regulatory compliance,
- Ensure that gaps and overlaps are identified and addressed, and
- Responsible for reviewing and monitoring the adherence to Information Security Management System (ISMS) policies and procedures.

Delivery Functions

Engineering

The Engineering team is responsible for software development and the actual production and building of the given product or service. They are the ones carrying out all the sprints and working on new or necessary features, updates, and fixes. Team is also responsible for testing and helps in making the product or service go live.

Product

Product team is responsible for defining the product vision and roadmap based on the market research, customer input and competitive analysis. In addition, Product management is also responsible for providing the direction to the engineering teams with regards to prioritization of product features, planning, developing, releasing the product/features, and providing active guidance for post deployment support. Product management is all about identifying the customer needs, market needs and delivering the product that have the ability to fulfill the customers' needs and requirements. The product team is also responsible for forecasting, budgeting, and collaborating with the marketing department on branding and GTM.

DevOps

The DevOps team is responsible for Automating. Responsibility of the DevOps team to automate tasks and improve the efficiency of engineering and IT. DevOps team is responsible for maintaining the Engineering tools. The culture of DevOps team leads to shared ownership, on-call responsibilities, and accountability for a team's underlying service.

Support Functions

Human Resources (HR)

The Human resources team at GupShup is responsible for strategically managing people as business resources. This includes managing recruiting and hiring employees / consultants, employee / consultant training and development, talent management through annual performance appraisal process and probation. The HR team at GupShup has defined its organizational structure, reporting lines, authorities, and responsibilities as a part of its internal organization and business model adopted to meet its organizational goals and objectives along with the commitments.

The HR team also supports employee engagement, employee welfare and ensures that adequate personnel with appropriate skill sets are made available within GupShup. Documented job descriptions for all GupShup's delivery and support functions have been defined and published within a Google Drive by the HR team.

Legal

The Legal team is responsible for preparing, modifying, and reviewing contractual agreements between GupShup, its vendors and customers. The legal team is also responsible for overall governance and regulatory compliance.

Finance

The Finance team is responsible for financial accounting and reporting, planning, organizing, tax compliance & reporting, management of cashflows, budgeting, forecasting, and ensuring there are sufficient funds available to meet the day-to-day payments.

Admin and Facilities

The Admin and Facilities team is responsible for administrative activities involving procurement, housekeeping, employee induction, physical security of the GupShup premises, installation, and maintenance of equipment for power backup, and for controlling environmental conditions including temperature and humidity.

Marketing

The Marketing team is responsible for creating awareness about GupShup's business, its products and providing inputs to its customers. The team is involved in monitoring the competitors, creating new ideas, identifying outlets, planning the strategy to involve customers, and retaining them.

Technical Support

The Technical support team is responsible for managing technical queries raised by the customers via ticketing tool or emails. They are the bridge between customer and internal product and engineering teams. The team is responsible to manage day-to-day internal and external issues by escalating it to vendors or internal teams.

Customer support

The Customer support team is responsible for any Support and Assistance required for Customers. Customer Support team is trained to help customers to the best of their knowledge for the plethora of products GupShup has to offer. We at L1 support work in a coordinated manner with other L2 level teams/Technical support team and ensure the resolutions/solutions of issues/concerns raised by our customers.

Sales

The Sales team is responsible for lead generation and to promote and sell products/services using solid arguments to existing and prospective customers. They are responsible for meeting the company's business's growth goals by selling products, services, or subscriptions.

Infrastructure Operations

The Infrastructure operations team is responsible for managing the entire Platform and its operational activity. This team manages deployment and operational activities of GupShup data center and cloud infrastructure. This team manages activities related to keeping the infrastructure optimal including backing up the systems, performance tuning, installing operating system upgrades, changes, and patches etc.

Site Reliability Engineering (SRE)

The SRE team is responsible for 24/7 monitoring of GupShup Infrastructure across the data center and cloud platforms. The SRE incident management team does the L1, L2 incident handling and escalation process.

Management Information System (MIS)/Internal-IT

The Management Information Systems (MIS) team is responsible for managing the end user computing (hardware, software, email, collaborative tools) systems and in-house office IT infrastructure services used for business-critical decision-making in the organization.

IT Security

The IT Security team executes the responsibility spanning over Governance, Risk, Compliance, Security Monitoring, Security testing, Security Operations and Data Privacy.

Policies and Procedures

GupShup has developed formal policies and procedures covering various areas such as company operations, human resources, finance, information technology, information security, business continuity management, change management and data privacy. The policies and procedures are available on the GupShup Google Drive which is accessible to all GupShup employees and consultants, in accordance with GupShup's goals and objectives to sustain its control environment. Any changes to the same are communicated to employees over email.

Policies and procedures are deemed to be accepted by the employees and consultants when they sign the employment offer and the Non-Disclosure Agreement (NDA) which includes clauses for exclusive employment, confidentiality, and period of effectiveness. It is digitally signed through DocuSign, and a report is generated which is sent across via email to the HR team.

Training and Awareness

On the day of joining, GupShup employees / consultants are given training on information security and are made aware of various policies like security incident management policy, password policy, Clear desk and clean screen policy, email communication, and data classification policy. Under the GupShup security incident management policy, employees / consultants are encouraged to promptly report any incident, breaches or lapses in the organization's compliance policies and procedure.

During the induction training program, the employees / consultants are also given training on dealing with disaster situations and are made aware of the topics such as threat, vulnerability, risk, data privacy, GDPR, data breach, user responsibility, email usage and exception handling. A quiz is carried out post the training session followed by feedback which is captured using a Google form.

Information Security Management System

GupShup has developed an organization-wide Information Security Management System (ISMS) Policy framework detailing the information security objective in alignment with the strategic direction of organization. The purpose of the Information Security Management System Policy is to establish the various security practices at GupShup and the ISMS Policy includes domains such as Access Control, Remote Access, Risk Management, Removable Media, HR Security, Asset Management, Asset Disposal, Physical and Environmental Security, Malware protection, Data Backup, Data Restoration, Data Retention, Data Protection, Cryptography, Password Management, Logging and Monitoring, Email Policy, Internet Policy, Network Security Policy, Vulnerability Management Policy, Patch Management Policy, Change Management Process, Secure Development Practices, Supplier Management Policy, Business Continuity Management Policy, Security Incident Management, Awareness Programs, Audit Management and Compliance Frameworks. The scope of this Policy document includes GupShup employees and consultants with access to the company assets, networks and other resources. Formal employee orientation programs are held to train all personnel on these policies upon recruitment and these policies are made available to GupShup employees and consultants on the GupShup Google Drive. GupShup reviews its ISMS policies on an annual basis or as and when necessary, i.e., when improvements to the ISMS process are identified. The internal and sustenance audits are conducted annually. The audits verify continuous compliance and sustenance of ISMS framework.

Business Continuity Management and Disaster Recovery

GupShup has developed an Application and Infrastructure related Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to minimize the effect of service disruption on GupShup's clients, staffs, assets, and information systems. BCP tests are conducted at

GupShup Delivery Centers to assess the preparedness of employees in the event of a disaster or severe incident. The tests include structured walkthroughs, simulation tests, emergency evacuation drills and tabletop session at defined periodicities.

Incident Management

GupShup has defined Data Breach and Incident Management policy for reporting and managing any information security, confidentiality, availability related incidents and to respond appropriately to any actual or suspected incidents affecting GupShup's information systems or its operations. The policy is made available on the Google Drive as a reference for all the GupShup employees. The details of the policy are also covered as part of the ISMS Awareness Training which is provided as part of the induction training conducted during the employee's onboarding. The security incidents are recorded, described, categorized based on the severity and analyzed for root cause. A JIRA Ticket is also raised and tracked to closure by the IT Security team through a Security Incident Management (SIM) Tracker in the Google Workspace. The IT Security team takes necessary preventive and corrective actions after analyzing the root cause of the incident. Post providing resolution to the reported security incidents, the learnings are shared across internally within GupShup either through the monthly information security awareness newsletters or through one-to-one emails pertaining to specific groups.

GupShup employees and consultants can report security incidents by writing an email with the incident details to "securityincident@GupShup.io". GupShup customers are informed about the incident reporting channels during the customer on-boarding phase. GupShup customers can report security incidents by writing an email with the incident details to "securitycompliance@GupShup.io". For Self-serve, customers can write to "DPO@GupShup.io". A JIRA Ticket is logged for all the reported security incidents.

Change Management

GupShup has defined Change Management process to regulate changes across infrastructure components and applications and for ensuring that changes are assessed, approved, tested, and implemented in a controlled manner.

Infrastructure related Change

Infrastructure related changes are any changes made to the infrastructure supporting the application servers. Changes requests for infrastructure changes are raised by requestor on JIRA tool, based upon internal requirements or request from customers. Infrastructure related change requests are reviewed and authorized by the corresponding Change Advisory Board (CAB) which comprises of members from the Supporting functions. All changes related to infrastructure go through a Quality Assurance process to ensure that all the requirements have been included and fulfilled effectively. Once the infrastructure related changes are approved in the Quality Assurance, changes are implemented by Engineering team and/or DevOps team as per the timeline. For changes impacting key clients, their account managers are notified so that they can inform the clients regarding the change and its implementation timeline. Once the infrastructure changes are successfully completed, the respective support function team Head reviews the effectiveness of the changes and approves the infrastructure changes. Once the approval from the respective Team Head is obtained, the infrastructure changes are implemented in production environment by the Infrastructure Operations team.

Application related Change

Change requests for customer applications hosted in third-party co-location datacenters are raised by the Product team or the Customer Support team based on the request from customer. Application related change requests are reviewed and authorized by Change Advisory Board (CAB) comprising of members from the ISMS Forum. The Product team creates a request on the JIRA Ticketing tool and shares the change requirements with the Engineering team and/or DevOps team for development. Once the application changes are developed, Engineering team and/or DevOps team performs the feature testing in validation environment and documents the test results in the JIRA Ticket. In case issues are identified during the feature testing, the Engineering team and/or DevOps team performs the corrective code changes, to the repositories for which they have access. Once the Feature testing is successfully completed, the team performs a manual security testing of the developed code in the QA environment. Post successful completion of Security testing, the team provides sign-off for moving the code to the User Acceptance Testing stage.

The change requestor or the Product team Manager performs the User Acceptance Testing in the QA environment and provides an email confirmation to the Engineering team and/or DevOps team. Once UAT is signed-off, the application changes are implemented in production environment by the Infrastructure Operations team.

Risk Assessment

GupShup recognizes that risk assessment is a critical component of its operations and is instrumental in ensuring its information systems and customer data are suitably managed and secured. GupShup has established an Asset-based Risk Assessment Methodology (comprising policies, and procedures) with an objective to establish an approach for managing information security risks, to reduce their impact and maximize the organization's ability to manage and maintain the acceptable level of risk. This methodology is applicable to all the various assets connected to information processing, storage, and transfer across GupShup.

GupShup has adopted the following risk assessment approach taking into consideration the business environment, size of the organization and the risks faced by the organization:

- Specification of company objectives
- Identification of information assets
- Identification of threats and vulnerabilities

- Threat and Vulnerability analysis
- Threat classification and assessment of the probability of occurrence
- Assets risk evaluation and determining the level of risk
- Development of a risk treatment plan

Risk Identification

The following activities are performed as part of risk identification:

- Identification and classification of information assets
- Identification of threats and vulnerabilities
- Identification and classification of incidents
- Assessment of probability of occurrence
- Assessment of impact

The risk score is calculated based on the level of consequences of the incidents and probability of occurrence of the threat.

Risk Treatment and Mitigation

The following activities are performed as part of risk treatment and mitigation:

- Analysis of root causes of identified risks
- Evaluation of common root causes and the consequences
- Assessment and prioritization of mitigation alternatives
- Selection and allocation of the resources required for specific risk mitigation alternatives

Risk Review

The risk register is created as part of risk treatment and mitigation exercise is reviewed and approved by the Associate Director, IT Security team, GupShup on an annual basis or whenever there is a change to the business environment.

Monitoring

GupShup's control monitoring framework involves the following:

Internal Audit

Internal Audits are conducted by the IT Security team for activities performed by the Product teams and other Support Functions, on an annual basis. IT Security team prepares an internal audit report documenting the issues of non-compliance and shares the internal audit report with Product team and other support Functions through emails. In case of any noted observations, the remediation measures are tracked to closure by IT Security team.

External Audit

GupShup is certified against ISO 27001:2013 standard by an independent audit agency.

Datacenter Audit

GupShup obtains SOC attestation reports from its third-party colocation datacenters on an annual basis and verifies that the risks associated to the services obtained are addressed adequately with the controls and processes implemented by the third-party colocation datacenters.

Vulnerability Assessments

On a monthly basis, an Infrastructure-level and application-level vulnerability assessment is performed by a third-party vendor using the Qualys Guard tool to assess the vulnerabilities and evaluate the associated risks to Corporate Applications.

On a bi-annual basis, Infrastructure penetration testing is performed, and an Application level Penetration Testing is performed annually by a third-party vendor to assess the vulnerabilities and evaluate the associated risks to the applications.

Network Monitoring

GupShup has configured the network devices and servers that are to be monitored for availability as per the Infrastructure Monitoring procedure within the Zabbix Infrastructure Monitoring tool.

Information

Information Technology Environment

Conversational Messaging Platform

Gupshup provides Conversational Messaging Platform for its clients to communicate SMS, Voice, Email, WhatsApp, and Bot based information to their customers. Gupshup facilitates the services by accepting input messages via APIs from its clients and delivering them to end users. The process is completely automated with no manual intervention. Gupshup has subscribed to Infrastructure as a Service (IaaS) from public cloud services provider Amazon Web Services (AWS) for its Conversational Messaging Platform (except for Voice and SMS channels). The production application servers operate on Ubuntu OS and the data associated to the platform is hosted on AWS Relation Database Service (RDS) and MySQL instances.

Bot Development Services

Gupshup provides Bot Platform to its clients which enables them to build intelligent chatbots and voice assistants that can be built once and deployed across various channels such as WhatsApp, Instagram, Twitter, Google Assistant, etc. Gupshup facilitates the services by providing bot building tools such as pre-built bot templates, cloud-based flow Builder to create conversation flow with a graphical editor as well as scripting tools. The

Bot Hosting Framework consists of an Integrated Development Environment (IDE) and Conversational User Interface (UI) Builder.

Applications and Tools

Following are some of the key applications and tools used by GupShup in the provision of their services:

S. No.	Application / Tool	Description
1	JIRA	JIRA is a ticketing service application used by the HR, MIS, SRE and Platform Engineering, Engineering & DevOps, Tech Support, and IT Security teams for planning, tracking and managing Security Incidents, Change and Service Requests.
2	Jenkins	Jenkins is an automation server used by the Engineering & DevOps team to build, test, and deploy changes to production.
3	Google Workspace	Google Workspace is a set of applications and tools used by GupShup employees for internal and external communication such as emails (Gmail), storage of documents (Google Drive), video conferencing (Google Meet), etc. offered by Google.
4	FreshDesk Ticketing Portal	FreshDesk ticketing portal is a ticketing portal used by Customer & Tech Support team to track and manage customer related queries and incidents.
5	Slack Messenger	Slack Messenger is an application used by all employees of GupShup as an internal instant messaging platform.
6	eScan Anti-virus	Anti-virus tool for providing Real-time protection, managing antivirus signature updates and periodic virus scans pertaining to GupShup desktops and laptops.
7	Google Data Loss Prevention (DLP)	Email monitoring tool provided by Google for monitoring emails that is sent and received by GupShup Domain on endpoint system.
8	Zabbix	Tool used for end-to-end infrastructure monitoring like CPU, memory, disk utilization etc., availability of infrastructure in third-party colocation datacenters and cloud.

S. No.	Application / Tool	Description
9	Corologix SIEM	Security Information Event Management tool is used for anomaly detection and alerting
10	FortiGate Firewall Solution	Corporate firewall used for restricting un-authorized access to GupShup domain within GupShup Delivery Centers.
11	DocuSign	Tool used for electronic signatures on legally binding contracts and all types of agreements.
12	GitLabEnterprise	Gitlab is a web-based repository hosting service used by the Engineering Team and/or DevOps team for source code and development projects. It provides access control and several collaboration features such as bug tracking, feature requests, task management and continuous integration.
13	Jira Service Management	A cloud-based software designed for incident response management and used by Incident Management and Site Reliability Team to improve reliability of GupShup's systems.
14	OCS Inventory	Open Computer and Software (OCS) Inventory tool is an asset management solution which enables users to scan and inventory IT assets.
15	Qualys Guard	Qualys Guard is a web-based vulnerability management tool to assess vulnerabilities and evaluate the associated risks to Corporate Applications.

Firewall

Firewall rules have been established on the corporate firewall to prevent unauthorized users from getting direct access to the GupShup network, using FortiGate Firewall Solution. They utilize the IPS / IDS component within their firewall to monitor and prevent any breaches and malicious attacks.

Intrusion Prevention System (IPS)

GupShup has enabled Intrusion Prevention System (IPS) and web filtering system on Firewall to prevent any unauthorized access, breaches, and attacks. Firewall logs are pushed to SIEM Corologix tool for monitoring purposes. GupShup is not responsible for the management and maintenance of network devices in third-party colocation datacenters.

Anti-Virus

eScan anti-virus software is installed and activated on all workstations (desktops and laptops) within GupShup environment and are updated with the latest antivirus signatures.

Communication

Internal Communication

Internal communication acts as an aid to help ensure adherence to policies and procedures. Messages pertaining to important corporate events, employee news and updates are communicated using electronic email. Email is also a means to draw attention of employees towards adherence to specific requirements pertaining to information security and business continuity. Communication with employees is maintained using Corporate G-mail, and Slack Messenger applications.

External Communication

External communication is critical to facilitate communication between customers and GupShup in order to track progress, and to identify and resolve issues, if any, on a timely basis. Communication with the customers is maintained using emails, the GupShup website, and telephone calls.

Components of the System Providing the Defined Services

Infrastructure

GupShup's infrastructure consists of workstations, domain controllers, firewalls, and internet connectivity used to connect to the GupShup network. GupShup manages the operating system for servers, network, and security devices and software such as anti-virus, network scanners, and log management applications. All core applications are hosted at the third-party colocation datacenters (NTT Netmagic and AWS).

GupShup provides its services to user entities using the infrastructure hosted on the third-party colocation datacenters at Amazon Web Services (AWS) and NTT Netmagic.

People

GupShup's Delivery teams provide services to its customers from Bangalore, Mumbai and Chennai. The delivery teams are recruited by GupShup based on resource requirements from various teams following their recruitment policies and procedures.

Policies and Procedures

GupShup has defined organization wide policies and procedures to ensure security, confidentiality, and availability of information and information systems. The policies and procedures are made available for all employees on a Google Drive for reference. GupShup ensures adherence to defined policies and procedures through internal audits, external audits, and awareness sessions.

Data

GupShup has defined an Information Classification and Handling Policy which defines data classification levels, protection requirements and access control mechanisms, and uploaded within a Google Drive which is accessible by all GupShup employees. GupShup as part of its ISMS policies and procedures has also established procedures for handling the Information shared by customers including its retention and disposal.

Criteria and Controls

The criteria for the Security, Availability and Confidentiality categories are organized into (a) the criteria that are applicable to all three categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the Security category. For the categories of Availability and Confidentiality a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the categories being reported on.

Common Criteria for Security, Availability and Confidentiality

A. Control Environment

GupShup has defined its organizational structure, reporting lines, authorities, and responsibilities as a part of its internal organization and business model adopted to meet its organizational goals and objectives along with the commitments.

GupShup operates under the directions of its Chief Executive Officer (CEO), Chief Technology Officer (CTO), Chief Product Officer, Chief Operating Officer (COO) and the Board of Directors (BoD) who constitute of the Chief Financial Officer (CFO) and the Finance Controller who are responsible for decision making and ensuring commitment to security, availability, and confidentiality at the entity level.

GupShup has segregated personnel and business functions into various departments comprising of delivery functions and support functions according to their job responsibilities as follows:

- Engineering team
- DevOps team
- Product team
- Infrastructure Operations team.
- Sales, Customer Success and Tech Support team
- Support Functions (includes Human Resources team, Marketing Team, IT Security team, Admin & Facilities team, MIS Team, Finance team and Legal team)

These teams are responsible and accountable for ensuring that GupShup's commitments and requirements as related to security, availability and confidentiality are fulfilled.

GupShup signs agreements with its vendors encompassing the integrity and ethical values to be upheld by them during lifecycle of the agreement. The agreement is signed by the relevant stakeholders from GupShup and the vendors.

Human Resources Practices

Prior to joining GupShup, a background verification (BGV) for the candidate is initiated by the HR team. A pre-BGV is performed by a third-party service provider to verify the employment details of the candidate. Once the pre-BGV is clear and the candidate is onboarded to GupShup, a post-BGV is performed by another third-party service provider to verify the following details:

- Education
- Prior Employment
- Address
- Court Records

As per the Hiring policies, candidates are required to have a minimum education qualification and experience based on the position and job requirements. In case, the candidate does not fulfill in the required criteria, their on-boarding process is halted.

As part of the on-boarding process, employees and consultants are required to acknowledge and sign an employee agreement regarding compliance with company policies, Anti Bribery and Money Laundering (AML) policies, Information Security Management Systems (ISMS) policies and Data Consent forms as it relates to the company's security and confidentiality requirements. Further, the employees and consultants are required to sign Non-Disclosure Agreement (NDA) which includes clauses for exclusive employment, confidentiality and period of effectiveness and breach of confidentiality. It is digitally signed, and a report is generated and sent across via email to the HR team.

During the induction training program, the employees / consultants are also given training on dealing with disaster situations and are made aware of the topics such as threat, vulnerability, risk, data privacy, GDPR, data breach, user responsibility, email usage and exception handling. A quiz is carried out post the training session followed by feedback which is captured using a Google form.

GupShup has defined and documented processes for the following, to ensure that personnel fulfil their responsibilities:

- Termination
- Probation
- Performance appraisal

B. Communication and Information

GupShup has established multiple channels of communication with its employees including the use of emails, Google Drive, Google Meet and Slack Messenger. The communications include but are not limited to communication of GupShup policies and procedures, corporate events, new initiatives, and training on information security and business continuity and disaster recovery procedures.

Information Security Management System (ISMS)

GupShup has developed an organization-wide Information Security Management System (ISMS) which includes designing, implementing, maintaining a coherent set of policies, processes, and guidelines based on International Organization for Standardization (ISO) 27001:2013 standard. The Chief Information Security Officer (CISO) is accountable for review of the ISMS policies, procedures and guidelines on an annual basis.

GupShup has defined policies and procedures within ISMS which includes Organization of Information Security, Human Resource security, Asset Management, Access Control, Cryptography, Physical and Environment Security, Operations Security, Communication Security, System Acquisition and Development, Supplier Relationships, Information Security Incident Management, Business Continuity Management, Compliance, Vulnerability Management policy and Data Protection policy. GupShup ISMS policies are updated by IT Security team and approved by the CISO on an annual basis. The GupShup policies and procedures relating to ISMS are stored on a Google drive and are made available with a view only access to all the GupShup employees for reference.

During the induction program, the new joiners are made aware of the various topics such as Threat, Vulnerability, Risk, Privacy, GDPR, Data Breach, User Responsibility, Email Usage, Security Incidents, Exception Handling, Myth and Reality. Attendance tracking is captured using a Google form.

As part of its Information Security awareness initiative the IT Security team sends out a Monthly Information Security Awareness email across the organization to impart security awareness to all its employees / consultants on a monthly basis.

Business Continuity Management System (BCMS)

GupShup has developed an Application and Infrastructure related Business Continuity Plan (BCP) to minimize the effect of service disruption on GupShup's clients, staffs, assets, and information systems. The following is documented in the BCP:

- Objective of the BCP
- Process for invocation of the BCP
- Roles and responsibilities in case of invocation of the BCP
- Process to be followed in case of invocation (such as communication, relocation)

- Process for the Business Impact Analysis (BIA)
- Testing to be performed periodically to assess the preparedness of employees in the event of a disaster or severe incident

The BCP is reviewed and approved by the Head of the department of Engineering and Operations on an annual basis.

Annually, a Business Impact Analysis (BIA) is carried out to identify potential threats that can impair system availability, and to assess the risks associated with the identified threats.

Periodic tests (such as structured walkthroughs, simulation tests, emergency evacuation drills and tabletop session) are conducted at GupShup Delivery Centers in Mumbai, Bangalore, and Chennai. The tests include the following:

- Fortnightly, mock DR Drills are carried out to test the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The details of the test are documented on a JIRA Ticket, which is then reviewed and approved by VP, IT
- Annually, a tabletop/walkthrough test is performed by the Engineering team and the results are reviewed and approved by the VP IT

Customer Agreements

GupShup and its customers agree and sign on the Master Service Agreement (MSA) consisting of the following:

- Scope of services, Program phase and Deliverables
- Suspension or termination of services
- Authorization and customer restrictions
- Customer obligations
- Confidentiality clauses
- Payment terms and Professional Services Rate Card
- Indemnification and limitation of liability clauses

The changes to the Master Service Agreement (MSA) are documented and maintained through an excel spreadsheet as Amendments and are signed by the GupShup CFO / Finance Controller and the relevant stakeholders from GupShup's customer.

GupShup has defined an MSA documenting the confidentiality requirements and clauses relating to non-disclosure and data protection for the services provided by the third-party colocation datacenter and cloud service provider. The MSA is signed by the relevant stakeholders from GupShup and third-party colocation datacenter and cloud service provider.

C. Risk Assessment

GupShup follows an asset-based methodology for conducting the risk assessment as defined in the Risk Assessment methodology document. The IT Security team identifies the possible risks to the organization by internal and external factors such as fraudulent reporting, possible loss of assets etc. And calculates the Risk Value based on the risk impact and probability of occurrence. The calculations are tabulated in a risk matrix format in the Information Security Risk Register. The Information Security Risk Register is stored on a Google drive and can only be accessed by the members of IT Security team. GupShup has also established a process for periodically reviewing and updating the risks controls if required.

The IT Security team prepares a risk treatment plan based on risk ratings/ net risk value which is documented in Risk Register and Residual Risk is calculated. The Residual Risk is reviewed and accepted by the Risk Owner based on the defined timeline.

As part of the annual information security risk assessment, the IT Security team reviews and updates the list of physical assets, information assets, software assets and intangibles in the risk register and performs the risk assessment as defined in the Risk Assessment methodology document.

As part of the annual information security risk assessment, the IT Security team captures results of the risk assessment in Management Response document which is shared with the CISO via email for the approval on final assessment report.

Further, the IT Security team uses the risks identified as per the risk assessment and treatment plan to develop the risk control matrix. The risk control matrix which assesses and monitor the changes in the business model, changes in leadership, changes in systems and technology and changes in vendor and business partner relationships.

GupShup has implemented the Internal Financial Controls framework covering the following: Control Environment, Risk Assessment, Control Activities, Information System and Communication, Monitoring.

D. Monitoring Activities

Compliance Monitoring

GupShup obtains Service Organization Controls (SOC) Reports from its third-party colocation datacenter and cloud service provider on an annual basis and verifies that the risks associated to the services obtained are addressed adequately with controls and processes implemented by the third-party colocation datacenter and cloud service provider.

Internal Audits

To monitor adherence to ISMS, the IT Security team performs internal audits of the GupShup delivery teams and support functions as per the Annual IA Programme Calendar. The IT Security team prepares an internal audit report documenting the issues of non-compliance and shares the internal audit report with the respective GupShup delivery teams and support functions through email. In case of any noted observations, the remediation measures are carried out by the respective GupShup delivery teams and support functions and the IT Security team monitors the timely closure of the observations

External Audits

GupShup is certified against ISO 27001:2013 standard and external assessments are performed by an independent audit agency.

Third-Party Risk Assessment

GupShup has established a process for performing a risk assessment during on boarding of third-party colocation datacenter and cloud service provider to verify their compliance with security, availability, and confidentiality requirements.

Vulnerability Assessments and Penetration Testing

On a monthly basis, an Infrastructure-level and application-level vulnerability assessment is performed by a third-party vendor using the Qualys Guard tool to assess the vulnerabilities and evaluate the associated risks to Corporate Applications.

On a bi-annual basis, Infrastructure penetration testing is performed, and an Application-level Vulnerability Assessment and Penetration Testing (VAPT) is performed annually by a third-party vendor to assess the vulnerabilities and evaluate the associated risks to the applications.

The Vulnerability Assessment & Penetration Testing (VAPT) results are documented within a report and shared with Operations team stakeholders.IT-Ops and Engineering teams carry out the remediation procedures and provide sign-offs.

The respective Vulnerability Assessment report are sent across to the Engineering and Infrastructure Operations team, detailing the Critical, High, Medium, and Low vulnerabilities. The corrective actions are performed by the Engineering and Infrastructure Operations team as per the defined SLA's.

Code review is performed by a third-party vendor on applications before go-live and relevant corrective actions are performed by the Engineering team for high severity issues. A remediation review is performed by the third-party vendor post completion of corrective actions.

Firewall Monitoring

Corologix SIEM Tool is configured to monitor the corporate firewalls for the risks related to security, availability, and performance. The corporate firewalls have been configured to send security events to the Corologix SIEM Tool. The Platform Engineering team monitors the event logs related to GupShup's corporate firewalls and performs the corrective actions in case of any noted observations.

GupShup performs a review of the rulesets enforced on the corporate firewall every quarter and corrective actions are taken in case of any noted deviations from the baseline.

Cloud Event Monitoring

On a daily basis, the IT Security team extracts the Cloud Compliance Report through Cloud Guard Dome 9 from AWS for monitoring the security parameters. The IT Security team analyses the Cloud Compliance Report and shares a weekly report with VP, Tech Operations and Senior Manager, IT Security. In case of any noted security incidents, the Engineering and Infrastructure Operations team raises a JIRA ticket and performs the corrective action in a timely manner.

Security Incident Monitoring

Security incidents are reported to the GupShup through the following mechanisms:

- By GupShup employees / consultants writing to the IT Security team via email (securityincident@GupShup.io)
- By GupShup enterprise customers writing to the Customer Support team via email (enterprise-support@GupShup.io) or via telephonic support available on GupShup's website
- By GupShup key account customers writing to the Customer Support team via email (premiumcare@GupShup.me) or via telephonic support available on GupShup's website

In the case of customer reported security incidents, the Customer Support team raises a Freshdesk ticket to the IT Security team documenting the details of the security incident. The reported security incidents are analyzed by the IT Security team and if the incident is noted as a security incident, the IT Security team documents the security incident's occurrence date, severity, description, reported date within the Security Incident Management (SIM) Tracker in the Google Workspace. Upon analysis, if it is noted that GupShup's customers are impacted by the security incident, then GupShup informs the customer within 2 hours from the reporting of the incident. A JIRA ticket is also logged for the security incident to monitor the timely closure as per the defined SLAs. Post the resolution of the security incident, the SIM tracker is updated with the closure date, root cause, corrective action, and status. Further, the resolution is documented on the JIRA ticket and corresponding Freshdesk ticket (if any) and the status is marked as closed.

Upon request from the customer, a Root Cause Analysis (RCA) is shared with the customer detailing the summary of the issues, root cause analysis and the corrective and preventive measures taken.

Antivirus Monitoring

On a daily basis, the MIS team extracts a report from e-Scan Anti-virus (AV) tool capturing the current application version and anti-virus signature being used for all the employee workstations and shares the report with the MIS team through email. The MIS team assesses the report, to identify workstations that are not up-to-date and performs the appropriate corrective measures in a timely manner.

E. Control Activities

Infrastructure Monitoring

GupShup monitors the availability and performance of its infrastructure using Zabbix infrastructure monitoring tool. Zabbix generates automated alerts in Slack tool in case of any deviation from the defined thresholds. Corrective actions if any are performed by the Engineering and Infrastructure Operations team and tracked to closure on JIRA.

Firewall Monitoring

Corologix SIEM Tool is configured to monitor the corporate firewalls for the risks related to security, availability, and performance. The corporate firewalls have been configured to send security events to the Corologix SIEM Tool. The Infrastructure Operations team monitors the event logs related to GupShup's corporate firewalls and performs the corrective actions in case of any noted observations.

GupShup performs a review of the rulesets enforced on the corporate firewall every quarter and corrective actions are taken in case of any noted deviations from the baseline.

Hardening Standards

On a quarterly basis, the Infrastructure Operations team reviews and updates the hardening standards enforced for the Linux servers, within the third-party colocation datacenter and AWS, as well as the Linux, MAC, and Windows operating systems installed on the workstations.

Policies and Procedures

GupShup policies and procedures are defined and are made available to all GupShup employees on the corporate Google Drive. The policies and procedures include the following:

Information Security Management System (ISMS)
GupShup has developed an organization- wide Information Security Management System (ISMS) which includes designing, implementing, maintaining a coherent set of policies, processes, and guidelines based on International Organization for Standardization (ISO) 27001: 2013 standard. The Chief Information Security Officer (CISO) is accountable for the review of the ISMS policies, procedures, and guidelines on an annual basis.

Business Continuity Management System (BCMS)
GupShup has developed an Application and Infrastructure related Business Continuity Plan (BCP) to minimize the effect of service disruption on GupShup's clients, staffs, assets, and information systems. The following is documented in the BCP:

- Objective of the BCP
- Process for invocation of the BCP
- Roles and responsibilities in case of invocation of the BCP
- Process to be followed in case of invocation (such as communication, relocation)
- Process for the Business Impact Analysis (BIA)
- Testing to be performed periodically to assess the preparedness of employees in the event of a disaster or severe incident

The BCP is reviewed and approved by the Head of the department of Engineering and Operations on an annual basis.

Information Security Policy

GupShup has defined an organization-wide Information Security Policy within its ISMS Policy document that covers the process of performing an assessment of the risks to GupShup's information systems on an annual basis or based on any technological and environmental changes. The policy document is reviewed and approved annually by the Chief Information Security Officer (CISO, GupShup).

Change Management Policy

GupShup has defined a Change Management Process within its ISMS Policy document to regulate changes across infrastructure components and applications for ensuring that changes are assessed, approved, tested, and implemented in a controlled manner.

Information Classification and Labelling Policy

GupShup has defined an organization-wide Data Classification and Handling Policy that covers areas such as data classification levels, labelling of assets, protection requirements and access control mechanisms. Data within GupShup information systems are classified in accordance with the defined Data Classification and Handling Policy.

Incident Management Policy

GupShup has defined Data Breach and Security Incident Management, and includes procedures for reporting, categorization, and resolution of security incidents. The policy is stored on a Google drive and is made available with a view only access to all the GupShup employees for reference. The agreements with customers include the information on where customers need to report incidents. Customers are informed about these procedures during the contracting phase.

Access Management Policy

GupShup has established an organization-wide Access Management policy within its ISMS policy, which includes areas such as physical access and logical access to GupShup environment, system and application access controls and password policy. The policy is stored on a Google drive and is made available with a view only access to all the GupShup employees for reference.

Asset Classification Policy

GupShup has established an Asset Classification policy within its ISMS Policy. Asset inventory is currently maintained using the OCS Inventory tool. A unique ID is assigned to each asset and is maintained within the OCS Inventory tool database. The policy is made available on the Google Drive for reference of all GupShup employees. Software assets are handled manually by IT Team, where pre-approved assets are installed in the system. Any additional software can be installed on request.

Handling of Customer Data

GupShup as part of its Data Classification and Handling Policy has established procedures for handling the Information shared by customers. Retention and disposal of customer data have been defined and documented in GupShup's Data Retention and Disposal Policy.

F. Logical and Physical Access controls

Physical Access Procedures

Physical Access to GupShup Premises

GupShup's Mumbai premise is restricted using biometric access control system and GupShup's Bangalore and Chennai premises are restricted to authorized personnel having valid photo identification (ID) cards, also used as access cards along with RFID authentication. All GupShup's premises are monitored 24/7 by security guards.

The entry and exit points of GupShup premises are monitored by the Admin & Facilities team on a continuous basis through CCTV cameras. The CCTV logs are retained for a period of 90 days. CCTV cameras undergo preventive maintenance at defined intervals as per the maintenance contract with the external vendor.

Granting of Physical Access to GupShup Premises

When an employee joins GupShup, the HR Team raises a JIRA ticket capturing the details of the employee marking the Admin & Facilities Team. Post receiving an intimation from the HR Team, the Admin & Facilities Team provisions a photo identification (ID) based access card to the employee.

Revocation of Physical Access to GupShup Premises

When an employee resigns, the HR Team raises a JIRA ticket capturing the employee exit checklist and the employee's last working date, marking the Admin & Facilities team. On the employee's last working day, the Admin & Facilities team revokes the employee's photo identification (ID) card, and the physical access provided (biometric or RFID) and confirms the same on employee's exit checklist.

Physical Access to Server Room

Physical access to the server room in Mumbai and Bengaluru office is maintained via a lock and key mechanism. Only authorized members from the MIS and Admin & Facilities teams are allowed access to the server room. A logbook is maintained, containing the list of personnel who have entered the server room.

Visitor Access Management

Security guards at the entry points are responsible for ensuring that the details of the visitor, such as visitor's name, contact person from GupShup, purpose for visit and entry time are recorded within the visitor logbook, before permitting entry to the GupShup premises and issuing the visitor badge. The security guard collects the visitor badge when the visitor leaves the GupShup premises.

Logical Access Procedures

Granting of access to the GupShup domain

When an employee joins GupShup, the HR team raises a JIRA ticket capturing the details of the employee marking the Admin & Facilities and MIS teams. Post receiving an intimation from the HR team, the Admin & Facilities team provisions the IT assets, and the MIS team grants access to the GupShup domain.

Revocation of access to the GupShup domain

When an employee resigns, the HR team raises a JIRA ticket capturing the employee exit checklist and the employee's last working date, marking the Admin & Facilities and MIS teams. On the employee's last working day, the Admin & Facilities team requisitions back the IT Assets and the MIS team revokes access to the GupShup domain.

Workstation Controls and Controls Related to Transmission, Movement, and Removal of Information

GupShup has established a domain controller for governing the access to GupShup Domain. Users authenticate to the GupShup Domain using their unique login credentials.

Default guest and anonymous login is disabled, and built-in administrator accounts are renamed, and password protected to ensure that administrative access is granted to only authorized members from the MIS team.

Local administrative rights on workstations within the GupShup environment are restricted to authorized personnel from the MIS team.

Removable media devices, such as Compact Disk (CD) drives, Universal Serial Bus (USB) mass storage devices, and Compact Disk – Read Only Memory (CDROM) readers are disabled on all workstations within GupShup.

Screensavers with appropriate wait time is enabled on all workstations. Access to modify screensaver settings is disabled on all workstations. Unattended workstations are locked within a stipulated time of inactivity by a password protected screensaver, enforced through the local group security policy settings.

GupShup has implemented a Clear Desk Policy to ensure that information is not left unattended on the employee's/consultant's desks during and after working hours.

GupShup has also implemented a Clear Screen Policy to ensure that no confidential information is placed on the screens of the desktop / laptop and to lock the screens when the employee / consultant steps away from their desktop/laptop.

Email attachments are scanned at the gateway to prevent infection from malicious software and programs using the Google Admin DLP. Relevant data protection rules are enabled through the Google Admin DLP to block the communication of Credit Card details, abuse words and PAN Card details within emails.

eScan anti-virus software is installed and activated on all workstations within GupShup environment and are updated with the latest antivirus signatures at regular predefined intervals.

GupShup has established Corporate group policy settings for its Domain Controllers in order to enable and enforce account and password policies such as password length, maximum password age, enforced password history, password expiry, password complexity requirements, and account lockout settings. Access to password and account lockout settings is disabled on all workstations.

GupShup has enabled corporate group policy settings on the Domain Controller used to manage its workstations within the corporate network with account lockout policy settings to limit attempts of malicious login or unauthorized access to its systems.

Access to internet is restricted using web filters and software can be installed only by Internal IT team with admin privileges.

GupShup users connect to the GupShup domain from remote locations through a secure VPN connection over internet.

Corologix SIEM Tool is configured to monitor the corporate firewalls for the risks related to security, availability, and performance.

The Infrastructure Operations team monitors the event logs related to GupShup's corporate firewalls and performs the corrective actions in case of any noted observations.

GupShup has enabled Intrusion Prevention System (IPS) and web filtering system on Firewall to prevent any unauthorized access, breaches, and attacks. Firewall logs are pushed to SIEM Corologix tool for monitoring purposes.

Administrative Access to Change Management tools

Administrative access to the Code Repository tool, GitLab is restricted to authorized members from the Engineering team.

Administrative access to the Code Build and Orchestration tool, Jfrog is restricted to authorized members from the Engineering team.

Administrative access to the code deployment tools, Jenkins is restricted to authorized members from the Engineering team.

Granting of user access to the change management tools

When a user requires access to the change management tools (GitLab, Jfrog, Jenkins) the user's reporting manager communicates the access request to the administrator of the tool by creating a JIRA ticket. Access is granted to the specific change management tool based on the request from the user's manager.

Revocation of user access to change management tools

If an employee/consultant is transferred to a different department which does not require the user access to change management tools. The employee's/consultant's access on change management tools is revoked by the tool administrator.

On the last working day, the employee / consultant obtains clearance through a No Objection Certificate (NOC) from all relevant departments as mentioned on the exit checklist. Exit checklist is sent across to all the support teams such as the Engineering & DevOps, HR, Finance, MIS (Operations), IT-Security and Admin & Facilities teams. The employee's/consultant's access on change management tools are revoked by the tool administrator (Engineering & DevOps team) prior to signing the exit checklist.

Review of user access to change management tools

Engineering team reviews the list of active users for GitLab once in 6 months to ensure access is restricted to authorized personnel. In case of any noted deviations, the necessary corrective actions are performed in a timely manner.

Administrator access to the Corporate Firewalls and Switches

Corporate firewall and switches rules have been established on corporate firewall to ensure administrative access is restricted to authorized employees from the Engineering team.

Review of Access to corporate network infrastructure

Engineering team reviews the list of network infrastructure administrators on a quarterly basis to ensure access is restricted to authorized personnel. In case of any noted deviations, the necessary corrective actions are performed in a timely manner.

Administrator access to the OCS Inventory Tool

Administrative access to the OCS Inventory tool is restricted to authorized personnel from the MIS team.

Administrator access to the Freshdesk Ticketing tool

Administrative access to the Freshdesk ticketing tool is restricted to authorized personnel from the GupShup Infrastructure Operations team.

Secure Connection to Third-party colocation datacenter

An encrypted site-to-site Virtual Private Network (VPN) tunnel has been established for enabling secure data transmission between GupShup Delivery Centers to the third-party colocation datacenter. The access to the servers and/or databases within the third-party colocation datacenter is restricted through specific rules configured within the Corporate Firewall.

The SRE and Infrastructure Operations team has implemented an internet facing Load Balancer for AWS Virtual Private Clouds (VPCs) in the production environment to manage the application load and restrict unauthorized access to VPCs.

Granting of VPN Access to Datacentre Environment

The GupShup Tech Support team member raises a JIRA ticket to Infrastructure Operations team for provisioning Virtual Private Network (VPN) access to the third-party colocation datacentre environments which are reviewed and approved by GupShup Project Managers.

Granting of user access to Production environment

When a user requires access to production environment, the user's reporting manager communicates the access request to the administrator by creating a JIRA ticket. Access is granted by Infrastructure Operations to production environment based on the request from the user’s manager.

Privileged and administrative access to the production environment is restricted to authorized personnel from the Infrastructure Operations team.

Granting of user access to AWS

When a user requires access to the AWS, the user's reporting manager communicates the access request to the administrator by creating a JIRA ticket. Access is granted by Infrastructure Operations to AWS based on the request from the user’s manager.

Privileged and administrative access to the AWS is restricted to authorized personnel from the Infrastructure Operations team.

Granting of Access to FTP Folders

The FTP folders have been segregated for each GupShup customer by enabling access restrictions on the customer folders.

GupShup customers request the Tech Support team for granting access to an FTP folder through email. The Tech Support team raises a JIRA Ticket capturing details of the email request and addresses it to the MIS team. The MIS team provisions access to the specific FTP folder and sends an email confirmation to the customer with the user ID and login link. Once the email confirmation is shared with the customer, the Tech Support team closes the JIRA Ticket.

Revocation of VPN access from Datacentre Environment

The users reporting Manager or MIS team basis on the requirement shall raise a Jira ticket to the Infrastructure operations team for Revoking VPN access from Datacentre Environment.

Revocation of access from AWS

The users reporting Manager or MIS team basis on the requirement shall raise a Jira ticket to the Infrastructure operations team for Revoking VPN access from AWS.

G. System Operations

GupShup has established procedures to detect and monitor vulnerabilities and anomalies in its infrastructure. In addition, GupShup has established organization-wide hardening standards for workstations, network devices, servers, and databases to provide a controlled operating environment and to prevent any unauthorized access to critical system resources.

Vulnerability Management

Vulnerability Assessment and Penetration Testing (VAPT)

On an annual basis, an application level Vulnerability Assessment & Penetration Testing (VAPT) is performed by a third-party vendor to assess the vulnerabilities and evaluate the associated risks to the applications.

The infrastructure level Vulnerability Assessment & Penetration Testing (VAPT) is performed on a Bi-annual basis and results are documented within a report and shared with Infrastructure Operations team stakeholders. Infrastructure Operations and Engineering teams carry out the remediation procedures and provide sign-offs.

On a monthly basis, application-Level and Infrastructure-level Vulnerability assessment is performed by third-party vendor using the Qualys Guard tool to assess the vulnerabilities and evaluate the associated risks to services.

The respective Vulnerability Assessment report are sent across to the Engineering and Infrastructure Operations team, detailing the Critical, High, Medium, and Low vulnerabilities.

The corrective actions are performed by the Engineering and Infrastructure Operations Team as per the defined SLA's.

Code review is performed by a third-party vendor on applications before go-live and relevant corrective actions are performed by the Engineering team for high severity issues. A remediation review is performed by the third-party vendor post completion of corrective actions.

Security Incident Management

Security incidents are reported to the GupShup through the following mechanisms:

- By GupShup employees / consultants writing to the IT Security team via email (securityincident@GupShup.io)
- By GupShup enterprise customers writing to the Customer Support team via email (enterprise-support@GupShup.io) or via telephonic support available on GupShup's website
- By GupShup key account customers writing to the Customer Support team via email (premiumcare@GupShup.me) or via telephonic support available on GupShup's website

In the case of customer reported security incidents, the Customer Support team raises a Freshdesk ticket to the IT Security team documenting the details of the security incident. The reported security incidents are analyzed by the IT Security Team and if the incident is noted as a security incident, the IT Security team documents the security incident's occurrence date, severity, description, reported date within the Security Incident Management (SIM) Tracker in the Google Workspace. Upon analysis, if it is noted that the GupShup's customers are impacted by the security incident, then GupShup informs the customer within 2 hours from the reporting of the incident. A JIRA ticket is also logged for the security incident to monitor the timely closure as per the defined SLAs. Post the resolution of the security incident, the SIM tracker is updated with the closure date, root cause, corrective action, and status. Further, the resolution is documented on the JIRA ticket and corresponding Freshdesk ticket (if any) and the status is marked as closed.

Upon request from the customer, a Root Cause Analysis (RCA) is shared with the customer detailing the summary of the issues, root cause analysis and the corrective and preventive measures taken.

GupShup employees / consultants are provided awareness on security incident management and security incident reporting during the induction training conducted on the date of joining.

GupShup customers are informed about the incident reporting channels during the customer on-boarding phase.

Data Loss Prevention (DLP)

GupShup has implemented Google Workspace Admin Data Loss Prevention (DLP) tool to monitor, detect, and alert if any sensitive or confidential data is sent out of GupShup network to external networks.

The DLP security notification is shared across to the affected individuals via mail and a JIRA Ticket is also logged for the security incident. The ticket is tracked down to closure as per the security incident process.

On a weekly basis, the IT Security team extracts the Cloud Compliance Report through AWS Security for monitoring the security parameters. The IT Security team analyses the Cloud Compliance Report and shares the weekly reports with Infrastructure Operations team

In case of any noted security incidents, the Engineering and Operations team raises a JIRA Ticket and performs the corrective action in a timely manner.

Patch Management

‘GupShup has established a patch management process through the Golden image approach. Infrastructure Operations team prepares a golden image based on the latest security benchmarks which is subjected to periodic vulnerability assessments and penetration testing to ensure the servers in production are hardened and free of vulnerabilities.

Patches are applied by authorized personnel from the Infrastructure Operations team as a process of upkeeping the golden image to the latest, tested by the Quality Assurance (QA) team and then deployed in the production environment based on appropriate approvals.

H. Change Management

GupShup has defined a Change Management Process within the ISMS Policy document to regulate changes across infrastructure components and for ensuring that changes are assessed, approved, tested, and implemented in a controlled manner. The Change Management process document contained within the ISMS Policy document is made available to all GupShup employees on the Google Drive for reference.

Change Authorization

Changes to be developed are communicated by the Product team to the Engineering team. The Product team creates a request on JIRA and shares the change requirements with the Engineering team.

Change requirements include customer requested changes, application feature changes and enhancements identified by the Product team.

Change Development

Each request created by the Product team is considered as an 'User Story' in JIRA. Each 'User Story' consists of multiple tasks and sub-tasks relating to customer requirements and application enhancements.

The developers make a copy of the Master Production trunk (the section after the last release went live) from the GitLab on their individual systems. This copy is referred to as the Develop branch.

Development is performed by developers on their individual systems on a section of the code of the Develop branch based on the requirements in the sprint.

Code Review

The developer raises a Pull Request on the GitLab once development is complete indicating that the code is ready for review before being tested by the QA team.

The developer selects the reviewers on the GitLab who get an email notification that the developed code is ready for their review. Reviewers review the code and provide comments against the modified/updated code if necessary.

Developers make modifications to the code if required based on the review and then re-submit the code changes on the Pull Request. Upon reviewing the modifications to the code, the reviewer approves and merges the code.

Change Testing - Feature Testing

Feature Test cases are defined by the developers at the beginning of the sprint cycle. Code that has been reviewed is ready for testing.

Feature testing of the developed code is performed by the developers on their systems by running automated unit tests. Code is considered ready for Security testing when results of all the unit test cases are green.

Change Testing - Security Testing

Once Feature testing is successfully completed, the QA team performs a manual security testing of the developed code in the QA environment.

After successful completion of Security testing, the QA team provides sign-off for moving the code to the Vulnerability and Load testing stage.

Change Testing - Vulnerability and Load Testing

A set of Vulnerability and Load test cases are executed by the QA team to focus on critical functionality and ensure the application can perform basic features to ensure high-level functionality. The results are documented on the JIRA ticket. A sign-off is provided by the QA team via email in case of successful testing or comments in case of issues noted.

Sign offs are also provided by the Tech Support and the Product Manager. Additionally, Ops team provides sign off in case of DB Changes.

Change Testing - UAT

User Acceptance Testing is not mandatory for all changes. When the Product team determines that UAT is required, it is performed by the Product Manager in the QA environment and sign-off is provided via email.

Migration to Production

GupShup has established a process to perform vulnerability scans of the developed code prior to the migration to production environment.

The vulnerabilities identified, if any are documented through a JIRA Ticket and necessary corrective actions are performed.

Change Deployment in Production

Based on code merged by the team lead, multiple jobs are automatically triggered on Jenkins to deploy the code in production environment. Access to change the trigger configuration on Jenkins is restricted to the administrator. The deployment is monitored for any failure and appropriate actions are taken.

Segregation of Duties

Segregation of duties has been enforced to ensure that only the Development team has access to check out code for development and only the Senior Team member from the Engineering & DevOps team have access to deploy the code into Production.

Segregation of Environment

GupShup has established different environments for Development, QA, and Production and has established controls to ensure segregation of production data from the Development and QA environment.

I. Risk Mitigation

Business Continuity Plan

GupShup has developed an Application and Infrastructure related Business Continuity Plan (BCP) to minimize the effect of service disruption on GupShup's clients, staffs, assets, and information systems. The following is documented in the BCP:

- Objective of the BCP
- Process for invocation of the BCP
- Roles and responsibilities in case of invocation of the BCP
- Process to be followed in case of invocation (such as communication, relocation)
- Process for the Business Impact Analysis (BIA)
- Testing to be performed periodically to assess the preparedness of employees in the event of a disaster or severe incident

The BCP is reviewed and approved by the Head of the department of Engineering and Operations on an annual basis.

Annually, a Business Impact Analysis (BIA) is carried out to identify potential threats that can impair system availability, and to assess the risks associated with the identified threats.

Periodic tests (such as structured walkthroughs, simulation tests, emergency evacuation drills and tabletop session) are conducted at GupShup Delivery Centers in Mumbai, Bangalore, and Chennai. The tests include the following:

- Fortnightly, mock DR Drills are carried out to test the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The details of the test are documented on a JIRA Ticket, which is then reviewed and approved by VP, IT
- Annually, a tabletop/walkthrough test is performed by the Engineering team and the results are reviewed and approved by the VP IT

Vendor Risk Management

GupShup has defined Supplier Relationship policies and procedures to ensure vendors are compliant with GupShup's information security requirements. On an annual basis, GupShup obtains SOC Reports from its third-party colocation datacenter and cloud service provider and verifies that the risks associated to the services obtained are addressed adequately with controls and processes implemented by the third-party colocation datacenter and cloud service provider.

J. Additional Criteria for Availability

Environmental Controls

The Admin & Facilities team maintains all GupShup facilities and supports equipment for controlling environmental conditions in GupShup premises.

Smoke detectors and fire alarms are installed in strategic locations in the premises and server room within GupShup. Fire extinguishers are located at key locations within the premises.

Preventive maintenance for smoke detectors, fire alarms, fire extinguishers, and fire suppression systems are performed on a yearly basis.

Power backup for the server room is provided through Uninterruptible Power Supply (UPS) systems and preventive maintenance is performed on a yearly basis.

Air-conditioners are installed inside the server room to control and maintain temperature and humidity conditions.

Business Continuity

GupShup has developed an Application and Infrastructure related Business Continuity Plan (BCP) to minimize the effect of service disruption on GupShup's clients, staffs, assets, and information systems. The following is documented in the BCP:

- Objective of the BCP
- Process for invocation of the BCP
- Roles and responsibilities in case of invocation of the BCP
- Process to be followed in case of invocation (such as communication, relocation)
- Process for the Business Impact Analysis (BIA)
- Testing to be performed periodically to assess the preparedness of employees in the event of a disaster or severe incident

The BCP is reviewed and approved by the Head of the department of Engineering and Operations on an annual basis.

Annually, a Business Impact Analysis (BIA) is carried out to identify potential threats that can impair system availability, and to assess the risks associated with the identified threats.

Periodic tests (such as structured walkthroughs, simulation tests, emergency evacuation drills and tabletop session) are conducted at GupShup Delivery Centers in Mumbai, Bangalore, and Chennai. The tests include the following:

- Fortnightly, mock DR Drills are carried out to test the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The details of the test are documented on a JIRA Ticket, which is then reviewed and approved by VP, IT

- Annually, a tabletop/walkthrough test is performed by the Engineering team and the results are reviewed and approved by the VP IT

Monitoring and Reporting

GupShup monitors the availability and performance of its infrastructure using Zabbix infrastructure monitoring tool. Zabbix generates automated alerts in Slack tool in case of any deviation from the defined thresholds. Corrective actions if any are performed by the Engineering and Infrastructure Operations team and tracked to closure on JIRA.

Backup and Restoration

Third Party Colocation Datacenter – Database Backup
A daily full backup of all the databases in production environments hosted in the third-party colocation datacenter is carried out using the Xtrabackup tool.

AWS Relational Database Backup
An automated weekly full backup is performed on the AWS Relational Database Services (RDS) instances and the backup logs are retained for a period of 7 days.

AWS AMI Instance Backup
The Amazon Machine Images (AMI) instance backups are performed on a daily basis using the policies configured in Amazon Data Lifecycle Manager. The AMI instance backups are retained for a period of 7 days.

Restoration Testing
Restoration testing of backups on AWS and third-party colocation datacenters is performed on a quarterly basis by the Infrastructure Operations team and the results are documented on a JIRA ticket.

AWS Server disaster recovery
The Infrastructure Operations team has configured Disaster Recovery policies to back up all active AMI instances during each backup to a segregated availability zone within Data Lifecycle Manager.

GupShup Uptime SLAs
GupShup has defined service uptime SLAs within the Master Service Agreement (MSA) signed with its customers and monitors and reports it on a continuous basis.

K. Additional Criteria for Confidentiality

Confidentiality Agreements

On the day of joining, the employees and consultants are required to sign GupShup's Non-Disclosure Agreement (NDA) which includes clauses for exclusive employment, confidentiality and period of effectiveness and breach of confidentiality. It is digitally signed through DocuSign, and a report is generated and sent across via email to the HR team.

GupShup has established procedures to classify and protect confidential information related to its own and its customers.

GupShup obtains customer consent prior to any changes which may result in a change in agreed and accepted confidentiality practices.

GupShup has defined an MSA documenting the confidentiality requirements and clauses relating to non-disclosure and data protection for the services provided by the third-party colocation datacenter and cloud service provider. The MSA is signed by the relevant stakeholders from GupShup and third-party colocation datacenter and cloud service provider.

Protection of Customer Data

GupShup customers are hosted in a dedicated Virtual LAN (VLAN) within the third-party colocation datacenter / AWS VPC. Customers can access the hosted applications via a dedicated URL through Hypertext Transfer Protocol Secure (HTTPS) internet protocol.

GupShup has established different Development, QA, and Production environments for Conversational Messaging Platform and Bot Development Services and has established controls to ensure segregation of production data from the Development and QA environments so that access to confidential information is appropriately restricted.

GupShup has established a process to destroy/erase/anonymize personal information records as specified in the Data Retention and Disposal policy using appropriate data destruction techniques.

Post the data retention period, destruction of relevant company data using appropriate data destruction techniques is carried out basis the existing statutory norms. A JIRA ticket is also raised which captures the data being destroyed/erased/anonymized.

GupShup has established a shredding process to dispose the physical hard copy data such as paper output containing personal information using the paper shredder.

Handling of Customer Data

GupShup as part of its Data Classification and Handling Policy has established procedures for handling the information shared by customers including its retention and disposal.

Clear Desk and Clear Screen

GupShup has implemented a Clear Desk Policy to ensure that information is not left unattended on the employee's /consultant's desks during and after working hours.

GupShup has also implemented a Clear Screen Policy to ensure that no confidential information is placed on the screens of the workstation and to lock the screens when the employee / consultant steps away from their workstation.

Information Classification and Labelling

GupShup has developed an organization wide Information Classification and Labelling Policy that covers areas such as data classification levels, labelling of assets, protection requirements and access control mechanisms. Data within GupShup information systems are classified in accordance with the defined Information Classification and Labelling Policy.

The Data transferred over a secure API accessed over the HTTPS. The Data at rest is stored using AES 256-bit encryption mechanism

Data stored in the production databases and S3 buckets are encrypted.

Trust Services Criteria and Controls

The Trust Services Criteria for security, availability, and confidentially and the controls that meet the criteria, while listed in the accompanying Trust Services Criteria, Controls are nevertheless an integral part of this description.

Description of Trust Service Criteria and Related Controls

Trust Services Criteria Mapping

The following mapping demonstrates how each of the controls described within the report addresses the criteria for the Security, Availability, and Confidentiality Trust Services Criteria. GupShup's controls can be found in the subsequent table.

Criteria	Criteria Description	Control Reference
CC1.0 – Common Criteria Related to Control Environment		
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	A04, A10, A08, B04
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	A01, A06, F25
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A01, B02, A09, F24
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A02, A03, A07, A08
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A01, A05, A06, A09, A10, F25
CC2.0 – Common Criteria Related to Communication and Information		
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	B07, B10, B15, B17, B22, B23, B24
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A02, B01, B02, B04, B05, B06, A05, B08, B11, A06, A07, A08, B12, B13, B14, F24, F25

CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	B02, B03, B04, B16, B17, B18, B19, B09, B20, B21
CC3.0 – Common Criteria Related to Risk Assessment		
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	C01, B08, A06, C07,
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.	C01, C02, C03, C04, C05, B10, C06, C08
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	C01, C02, B08
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	B24, C07, C08, C01
CC4.0 – Common Criteria Related to Monitoring Activities		
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	B07, C03, C04, C05, B10, D01, D02, C06, B15, D03, D04, D05, D06, D07, B17, B22, B24, D08, D09, D10
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	B07, C04, C05, B10, D01, B22, D09
CC5.0 - Common Criteria Related to Control Activities		
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	E03, C02, C06, D08, C07, C08
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	E01, E02, E04, E05, E06, E07, B06, B11, C06, E10, E11, E12, D03, D06, D07, D08, E13, E14, B16, E15, E16, E17, E18, E19, D10

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A02, A03, B01, B02, B03, B04, B05, E01, E04, E05, E06, B06, E08, A05, C01, C02, B08, B11, A06, E09, A08, B12, B14, E15, E16, F24
CC6.0 - Common Criteria Related to Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	F01, F02, F06, F09, E01, F10, F12, E02, E04, E05, E06, F15, F16, E07, F17, D06, F20, D07, D08, E13, E14, E15, E16, F21, F22, F23, E17, F25, F26, F27, F28, D10, F30, F31, F32, F33
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	F01, F02, F15, F16, E07, F17, F21, F22, F29, F30, F31, F32, F33
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity’s objectives.	F01, F02, E01, F10, E04, E05, E06, F15, F16, F17, D06, D10, E14, E15, E16, F21, F22, F31, F32, F33
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.	F03, F04, F05, F06, F07, F08, F29
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.	B20, B21

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	F14, F18, F19, D05, F20, E13, F24, E17, F27
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	F11, F18, F24
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	D04, F13, F14, F19, F24
CC7.0 - Common Criteria Related to System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	F13, G02, C04, C05, B10, F19, D04, D05, D08
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	F13, F18, G02, B09, G03, C04, C05, B12, D05, B18, F24
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	G01, G02, F01, G03, B12, B18, B09, E18,
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	G02, B09, G03, B18
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	B06, E08, G02, B09, G04, E18

CC8.0 – Common Criteria Related to Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	H01, H02, H03, H04, H05, H06, H07, H08, H09, E03, D03, H10, H11, H12
CC9.0 – Common Criteria Related to Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	B08, C01, C02, C07, G01
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	B02, B03, C06
Additional Criteria for Availability		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	F25, J05
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	J01, J02, J03, J04, E10, E11, E12, G04, E18, E19, J05
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	E08, G01, G04
Additional Criteria for Confidentiality		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	B02, B03, B04, B14, B23, D03, F18, F24, H12, K01
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	B14, B20, B21

Common Criteria Related to Control Environment

Control Reference	Mapped Criteria	Controls specified by GupShup
Organization Management		
A01	CC1.2 CC1.3 CC1.5	GupShup has defined its organizational structure, reporting lines, authorities, and responsibilities as a part of its internal organization and business model adopted to meet its organizational goals and objectives along with the commitments.
A09	CC1.3 CC1.5	GupShup has segregated personnel and business functions into various departments comprising of product teams and other support functions according to their job responsibilities as follows: Engineering team DevOps team Product team Sales, Customer Success and Tech Support team Support Functions (includes Human Resources team, Marketing team, IT Security team, Admin & Facilities team, MIS team, Finance team and Legal team) These teams are responsible and accountable for ensuring that GupShup's commitments and requirements as related to security, availability, and confidentiality are fulfilled.
A10	CC1.1 CC1.5	GupShup signs agreements with its vendors encompassing the integrity and ethical values to be upheld by them during lifecycle of the agreement. The agreement is signed by the relevant stakeholders from GupShup and the vendors.

Control Reference	Mapped Criteria	Controls specified by GupShup
Complementary Subservice Organization Control #1 The vendors are responsible to ensure the commitments to integrity and ethical values are upheld as per the agreements signed with GupShup.		
Information Security Management System (ISMS)		
A06	CC1.2 CC1.5 CC2.2 CC3.1 CC5.3	GupShup has developed an organization-wide Information Security Management System (ISMS) which includes designing, implementing, maintaining a coherent set of policies, processes, and guidelines based on International Organization for Standardization (ISO) 27001:2013 standard. The Chief Information Security Officer (CISO) is accountable for review of the ISMS policies, procedures and guidelines on an annual basis.
A07	CC1.4 CC2.2	As part of its Information Security awareness initiative the IT Security team sends out a Monthly Information Security Awareness email across the organization to impart security awareness to all its employees / consultants on a monthly basis.
Human Resource Practices		
A02	CC1.4 CC2.2 CC5.3	GupShup has defined and documented processes for the following, to ensure that personnel fulfil their responsibilities: Termination Probation Performance appraisal

Control Reference	Mapped Criteria	Controls specified by GupShup
A03	CC1.4 CC5.3	Prior to joining GupShup, a background verification (BGV) for the candidate is initiated by the HR team. A pre-BGV is performed by a third-party service provider to verify the employment details of the candidate. Once the pre-BGV is clear and the candidate is onboarded to GupShup, a post-BGV is performed by another third-party service provider to verify the following details: Education Prior Employment Address Court Records As per the Hiring policies, candidates are required to have a minimum education qualification and experience based on the position and job requirements. In case, the candidate does not fulfill in the required criteria, their on-boarding process is halted.
B01	CC2.2	As part of the on-boarding process, GupShup employees and consultants are required to acknowledge and sign an employee agreement regarding compliance with company policies, Anti Bribery and Money Laundering (AML) policies, Information Security Management Systems (ISMS) policies and Data Consent forms as it relates to the company's security and confidentiality requirements.
Technical Trainings		

Control Reference	Mapped Criteria	Controls specified by GupShup
A08	CC1.4 CC2.2 CC5.3	During the induction training program, the employees / consultants are also given training on dealing with disaster situations and are made aware of the topics such as threat, vulnerability, risk, data privacy, GDPR, data breach, user responsibility, email usage and exception handling. A quiz is carried out post the training session followed by feedback which is captured using a Google form.

Common Criteria Related to Communication and Information

Control Reference	Mapped Criteria	Controls specified by GupShup
Customer Agreements		
B02	CC1.3 CC2.2 CC2.3 CC5.3 CC9.2 C1.1	GupShup and its customers agree and sign on the Master Service Agreement (MSA) consisting of the following: Scope of services, Program phase and Deliverables Suspension or termination of services Authorization and customer restrictions Customer obligations Confidentiality clauses Payment terms and Professional Services Rate Card Indemnification and limitation of liability clauses
B03	CC2.3 CC5.3 CC9.2 C11	The changes to the Master Service Agreement (MSA) are documented and maintained through an excel spreadsheet as Amendments and are signed by the GupShup CFO / Finance Controller and the relevant stakeholders from GupShup's customer.
Complementary User Entity Control #1 User organizations are responsible for communicating changes to the MSA and for reviewing and signing-off on the changes.		
Information Security Management System		

Control Reference	Mapped Criteria	Controls specified by GupShup
E09	CC5.3	GupShup has defined policies and procedures within ISMS which includes Organization of Information Security, Human Resource security, Asset Management, Access Control, Cryptography, Physical and Environment Security, Operations Security, Communication Security, System Acquisition and Development, Supplier Relationships, Information Security Incident Management, Business Continuity Management, Compliance, Vulnerability Management policy and Data Protection policy. GupShup ISMS policies are updated by IT Security team and approved by the CISO on an annual basis. The GupShup policies and procedures relating to ISMS are stored on a Google drive and are made available with a view only access to all the GupShup employees for reference.
Business Continuity Management System		
B06	CC2.2 CC5.2 CC5.3 CC7.5	GupShup has developed an Application and Infrastructure related Business Continuity Plan (BCP) to minimize the effect of service disruption on GupShup's clients, staffs, assets, and information systems. The following is documented in the BCP: Objective of the BCP Process for invocation of the BCP Roles and responsibilities in case of invocation of the BCP Process to be followed in case of invocation (such as communication, relocation) Process for the Business Impact Analysis (BIA) Testing to be performed periodically to assess the preparedness of employees in the event of a disaster or severe incident

Control Reference	Mapped Criteria	Controls specified by GupShup
		The BCP is reviewed and approved by the Head of the department of Engineering and Operations on an annual basis.
Cloud Event Monitoring		
B07	CC2.1 CC4.1 CC4.2	On a daily basis, the IT Security team extracts the Cloud Compliance Report through Cloud Guard Dome 9 from AWS for monitoring the security parameters. The IT Security team analyses the Cloud Compliance Report and shares a weekly report with VP, Tech Operations and Senior Manager, IT Security. In case of any noted security incidents, the Engineering and Infrastructure Operations team raises a JIRA ticket and performs the corrective action in a timely manner.
Customer Communication		
B15	CC2.1 CC4.1	The Customer Support team (L1 Support) creates a Freshdesk ticket detailing the query/incident reported by a GupShup customer. The Customer Support team additionally creates a JIRA ticket assigned to the SRE/Infrastructure Operations team for the resolution the incident. Post the resolution of the incident, the JIRA and Freshdesk tickets are tracked to closure by the Tech Support and SRE/ Infrastructure Operations teams respectively.

Control Reference	Mapped Criteria	Controls specified by GupShup
Complementary User Entity Control #2 User organization is responsible for communicating the incident/query to GupShup via email and for confirmation of the resolution of incident/query.		
B17	CC2.1 CC2.3 CC4.1	Tech support team is responsible for sharing customer reports with the authorized personnel from the customer's end and for performing a Root Cause Analysis (RCA) for reported incidents. The customer report contains details of service requests, incidents, change request and problem management cases.
Complementary User Entity Control #3 User organizations are responsible for reviewing the customer reports containing details of service requests, incidents, change request and problem management cases.		
Antivirus Monitoring		
B22	CC2.1 CC4.1 CC4.2	On a daily basis, the Infrastructure Operations team extracts a report from e-Scan Anti-virus (AV) tool capturing the current e-Scan version being used and the latest scan date for all the employee workstations and shares the report with the Infrastructure Operations team through email.
Compliance Review		
B10	CC2.1 CC3.2 CC4.1	IT Security team shares a monthly Information Security Dashboard with the VP, TechOps capturing the following details: Trend of security incidents

Control Reference	Mapped Criteria	Controls specified by GupShup
	CC4.2 CC7.1 CC7.2	Remediation of vulnerabilities corresponding to the Vulnerability Assessment and Penetration Testing (VAPT) Tickets handled by the IT Security team Audit Management - External Audit Findings and Closure status
Service Levels		
B19	CC2.3	High and Urgent priority Freshdesk tickets are resolved within 2 hours from the reporting time and Medium and Low priority Freshdesk tickets are resolved within 4 hours from the reporting time as per the defined SLA's. The Freshdesk ticket status is updated as "Resolved" post providing the resolution to GupShup's customer.

Common Criteria Related to Risk Assessment

Control Reference	Mapped Criteria	Controls specified by GupShup
Risk Assessment Methodology		
C01	CC3.1 CC3.2 CC3.3 CC3.4 CC5.3	GupShup follows an asset-based methodology for conducting the risk assessment as defined in the Risk Assessment methodology document. The IT Security team identifies the possible risks to the organization by internal and external factors such as fraudulent reporting, possible loss of assets etc. and calculates the Risk Value based on the risk impact and probability of occurrence. The calculations are tabulated in a risk matrix format in the Information Security Risk Register. The Information Security Risk Register is stored on a Google drive and can only be accessed by the members of IT Security team.
C07	CC3.1 CC3.4 CC5.1	As part of the annual information security risk assessment, the IT Security Team is responsible for reviewing and updating the physical assets, information assets, software assets and intangibles. The Risk Assessment register defines the internal controls, treatment, risk owner, treatment result, level of vulnerability and finally a risk impact score is calculated.
B08	CC2.2 CC3.1 CC3.3 CC5.3	As part of the annual information security risk assessment, the IT Security team captures results of the risk assessment in Management Response document which is shared with the CISO via email for the approval on final assessment report.

Control Reference	Mapped Criteria	Controls specified by GupShup
B24	CC2.1 CC3.4 CC4.1	The IT Security team subscribes to technology and regulatory alerts from various vendors for monitoring of environmental, regulatory, and technological changes that may affect GupShup's Information System.
Risk Control Matrix		
C08	CC3.2 CC3.4 CC5.1	The IT Security team uses the risks identified as per the risk assessment and treatment plan to develop the risk control matrix. The risk control matrix assesses and monitors the changes in business model, changes in leadership, changes in systems and technology and changes in vendor and business partner relationships.

Common Criteria Related to Monitoring Activities

Control Reference	Mapped Criteria	Controls specified by GupShup
Vulnerability Assessment & Penetration Testing (VAPT)		
C03	CC3.2 CC4.1	On a monthly basis, an Infrastructure-level and application-level vulnerability assessment is performed by a third-party vendor using the Qualys Guard tool to assess the vulnerabilities and evaluate the associated risks to Corporate Applications. On a bi-annual basis, Infrastructure penetration testing is performed, and an Application level Penetration Testing is performed annually by a third-party vendor to assess the vulnerabilities and evaluate the associated risks to both infrastructure and applications.
C04	CC3.2 CC4.1 CC4.2 CC7.1 CC7.2	The Vulnerability Assessment report are sent across to the Engineering and Infrastructure Operations team, detailing the Critical, High, Medium, and Low vulnerabilities. The corrective actions are performed by the Engineering and Operations Team as per the defined SLA's.
Internal Audit		
D01	CC4.1 CC4.2	To monitor adherence to ISMS, the IT Security team performs internal audits of the GupShup delivery teams and support functions as per the Annual IA Program Calendar. The IT Security team prepares an internal audit report documenting the issues of non-compliance and shares the internal audit report with the respective

Control Reference	Mapped Criteria	Controls specified by GupShup
		GupShup delivery teams and support functions through email. In case of any noted observations, the remediation measures are carried out by the respective GupShup delivery teams and support functions and the IT Security team monitors the timely closure of the observations.
External Audit		
D02	CC4.1	GupShup is certified against ISO 27001:2013 standard and external assessments are performed by an independent audit agency.
B24	CC2.1 CC3.4 CC4.1	The IT Security team subscribes to technology and regulatory alerts from various vendors for monitoring of environmental, regulatory, and technological changes that may affect GupShup's Information System.
D09	CC4.1 CC4.2	Code review is performed by a third-party vendor on applications before go-live and relevant corrective actions are performed by the Engineering team for high severity issues. A remediation review is performed by the third-party vendor post completion of corrective actions.

Common Criteria related to Control Activities

Control Reference	Mapped Criteria	Controls specified by GupShup
Access Management		
B05	CC2.2 CC5.3	GupShup has established an organization-wide Access Management policy which includes areas such as physical access and logical access to GupShup environment, system and application access controls and password policy. The policy is stored on a Google drive and is made available with a view only access to all the GupShup employees for reference.
A05	CC1.5 CC2.2 CC5.3	GupShup IT Security reviews the third-party reports for security, confidentiality and availability management and maintenance of infrastructure of the third-party colocation data centers and cloud service provider.
Clear Desk & Clear Screen		
B11	CC2.2 CC5.2 CC5.3	**Clear Desk and Clear Screen** GupShup has implemented a Clear Desk Policy to ensure that information is not left unattended on the employee's/consultant's desks during and after working hours.

Control Reference	Mapped Criteria	Controls specified by GupShup
		GupShup has also implemented a Clear Screen Policy to ensure that no confidential information is placed on the screens of the desktop/laptop and to lock the screens when the employee /consultant steps away from their desktop/laptop.
B12	CC2.2 CC5.3 CC7.2 CC7.3	GupShup has established Security Incident Management policy within its ISMS, and includes procedures for reporting, categorization, and resolution of security incidents. The policy is stored on a Google drive and is made available with a view only access to all the GupShup employees for reference.
B13	CC2.2	GupShup has defined and documented a data classification policy which defines data classification levels, protection requirements and access control mechanism. The policy is stored on a Google drive and is made available with a view only access to all the GupShup employees for reference.
E10	CC5.2 A1.2	GupShup monitors the availability and performance of its infrastructure using Zabbix infrastructure monitoring tool. Zabbix generates automated alerts in Slack tool in case of any deviation from the defined thresholds. Corrective actions if any are performed by the Engineering and Platform team and tracked to closure on JIRA.
Server Hardening		
D03	CC4.1 CC5.2	GupShup has established a server hardening process. Infrastructure Operation team prepares a golden image based on the latest security benchmarks and servers are hardened with the golden image before deployment.

Control Reference	Mapped Criteria	Controls specified by GupShup
	CC8.1 C1.1	Patches are applied by authorized personnel from the Infrastructure Operation team as a process of upkeeping the golden image to the latest, tested by the QA Team and then deployed in the production environment based on appropriate approvals.
B23	CC2.1 C1.1	The Platform Team maintains a list of pre-validated Amazon Machine Images (AMI) known as Golden Images from which they spin up EC2 instances based on the requirement.

Common Criteria Related to Logical and Physical Access Controls

Control Reference	Mapped Criteria	Controls specified by GupShup
IT Asset Management		
F01	CC6.1 CC6.2 CC6.3 CC7.3	When an employee joins GupShup, the HR Team raises a JIRA ticket capturing the details of the employee marking the Admin & Facilities and MIS teams. Post receiving an intimation from the HR Team, the Admin & Facilities Team provisions the IT Assets and the MIS Team grants access to the GupShup domain.
F02	CC6.1 CC6.2 CC6.3	When an employee resigns, the HR Team raises a JIRA ticket capturing the employee exit checklist and the employee's last working date, marking the Admin & Facilities and MIS teams. On the employee's last working day, the Admin & Facilities Team requisitions back the IT Assets and the MIS Team revokes access to the GupShup domain.
Access Control System		
F03	CC6.4	GupShup premises are enabled with biometric access control systems and manned security guards are present at each entry and exit. Physical access within the GupShup premises is restricted to authorized personnel having valid photo identification (ID) cards.
Complementary Subservice Organization Control #2 Subservice organizations are responsible for restricting the physical access to their premises to authorized personnel.		

Control Reference	Mapped Criteria	Controls specified by GupShup
F04	CC6.4	Security guards present at the entry points of the GupShup premises are responsible for ensuring that details of a visitor, such as visitor's name, contact person from GupShup, purpose of the visit and entry time are recorded within the visitor logbook, before permitting entry to the GupShup premises.
F05	CC6.4	The entry and exit points of GupShup premises are monitored by the Admin & Facilities Team on a continuous basis through CCTV cameras. The CCTV logs are retained for a period of 90 days.
Complementary Subservice Organization Control #3 Subservice organizations are responsible for monitoring their physical premises through CCTV cameras.		
F06	CC6.1 CC6.4	Physical access to the server room is maintained via a lock and key mechanism. Only authorized members from the MIS and Admin & Facilities teams are allowed access to the server room. A logbook is maintained, containing the list of personnel who have entered the server room.
Complementary Subservice Organization Control #4 Subservice organizations are responsible for restricting the physical access to the server rooms to authorized personnel.		
F07	CC6.4	Granting of Physical Access to GupShup Premises

Control Reference	Mapped Criteria	Controls specified by GupShup
		When an employee joins GupShup, the HR Team raises a JIRA ticket capturing the details of the employee marking the Admin & Facilities. Post receiving an intimation from the HR Team, the Admin & Facilities Team provisions a photo identification (ID) card to the employee.
F08	CC6.4	**Revocation of Physical Access to GupShup Premises** When an employee resigns, the HR Team raises a JIRA ticket capturing the employee exit checklist and the employee's last working date, marking the Admin & Facilities. On the employee's last working day, the Admin & Facilities Team requisitions back the employee's photo identification (ID) card and confirms the same on employee's exit checklist.
F09	CC6.1	**Domain Controller** GupShup has established a domain controller for governing the access to GupShup Domain. Users authenticate to the GupShup Domain using their unique login credentials.
E01	CC5.2 CC5.3 CC6.1 CC6.3	**Guest Accounts and Default Administrator Accounts** Default guest login is disabled, and built-in administrator accounts are renamed, and password protected to ensure that the administrative access is restricted to authorized members from the MIS Team.

Control Reference	Mapped Criteria	Controls specified by GupShup
F10	CC6.1 CC6.3	**Local Administrative rights on desktops and laptops** Local administrative rights on workstations (desktops and laptops) are provided to the authorized members from MIS Team.
F11	CC6.7	**Removable Media and USB Storage Access** USB storage access and removable media devices, such as Compact Disk drives and Universal Serial Bus (USB) mass storage devices are disabled on all workstations (desktops and laptops).
F12	CC6.1	**Screen Saver** Screensavers with appropriate wait time is enabled on all workstations (desktops and laptops). Access to modify screensaver settings is disabled on all workstations.
F13	CC6.8 CC7.1 CC7.2	**Anti-virus Software** E scan anti-virus software is installed and activated on all workstations (desktops and laptops) within GupShup environment and are updated with the latest antivirus signatures.

Control Reference	Mapped Criteria	Controls specified by GupShup
F14	CC6.6 CC6.8	**Access to Internet** Access to internet is restricted using web filters within the GupShup environment when connected to GupShup VPN, and the ability to install software is restricted to the authorized members from MIS team. Employees connect to the GupShup domain from remote locations through a secure VPN connection over internet.
E02	CC5.2 CC6.1	**Password Control and Account Lockout on GupShup Domain** GupShup has established corporate group policy settings for its Domain Controllers in order to enable and enforce account and password policies such as password length, maximum password age, enforced password history, password expiry, password complexity requirements, and account lockout settings. Access to password and account lockout settings is disabled on all workstations.
E04	CC5.2 CC5.3 CC6.1 CC6.3	**Administrative access on Code Repository Tool/s** Administrative access on Code Repository tool, GitLab is restricted to authorized members from the Engineering Team.

Control Reference	Mapped Criteria	Controls specified by GupShup
E05	CC5.2 CC5.3 CC6.1 CC6.3	**Administrative access on Code Build and Orchestration Tool/s** Administrative access on Code Build and Orchestration tool, GitLab are restricted to authorized members from the Engineering Team.
E06	CC5.2 CC5.3 CC6.1 CC6.3	**Administrative access on Code Deployment Tools** Administrative access on code deployment tool, GitLab is restricted to authorized members from the Engineering Team.
F15	CC6.1 CC6.2 CC6.3	**Granting of user access to the change management tools** Access to the change management tool is provided to an employee by the respective tool's administrator, upon intimation of the required access by the employee's reporting manager through JIRA.
F16	CC6.1 CC6.2 CC6.3	**Revocation of user access to change management tools** On the last working day, the employee/consultant obtains clearance from all relevant departments including Engineering, Human Resources, Admin & Facilities, and MIS Teams on an exit checklist. Consecutively, a JIRA

Control Reference	Mapped Criteria	Controls specified by GupShup
		ticket is raised by the HR Team capturing the exit checklist containing the list of application-level accesses to be revoked.
E07	CC5.2 CC6.1 CC6.2	**Review of user access to change management tools** GupShup's Operations Team reviews the list of active users with respect to the change management tools every month and ensures that access is restricted to authorized personnel. In case of any noted deviations, the necessary corrective actions are performed in a timely manner.
F17	CC6.1 CC6.2 CC6.3	**Granting of user access to the production environment** When a user requires access to the production environment, the user's reporting manager communicates the access request to the administrator by creating a JIRA ticket. Access is granted to the production environment based on the request from the user's manager.
D06	CC4.1 CC5.2 CC6.1 CC6.3	**Review of access to corporate network infrastructure** The Platform Engineering Team reviews the list of network infrastructure administrators on a monthly basis and ensures that access is restricted to authorized personnel from the Platform Engineering Team. In case of any noted deviations, the necessary corrective actions are performed in a timely manner.

Control Reference	Mapped Criteria	Controls specified by GupShup
F20	CC6.1 CC6.6	GupShup users connect to the GupShup domain from remote locations through a secure VPN connection over internet.
D07	CC4.1 CC5.2 CC6.1	IT Security team performs a quarterly review of the ruleset configuration on the corporate firewall and corrective actions are taken in case of any noted deviations.
D08	CC4.1 CC5.1 CC5.2 CC6.1 CC7.1	GupShup has established a process to perform a review of the security configurations and hardening standards enforced on corporate environment every 6 months and corrective actions are taken in case of any noted deviations.
Complementary Subservice Organization Control #5 Third party colocation datacenter and cloud service provider are responsible for performing the hardening procedures for their network devices.		
E13	CC5.2 CC6.1 CC6.6	Corporate firewall and switches rules have been established on corporate firewall to ensure administrative access is restricted to authorized employees from the Engineering team.

Control Reference	Mapped Criteria	Controls specified by GupShup
E14	CC5.2 CC6.1 CC6.3	Administrative access on the corporate firewalls and switches are restricted to authorized personnel from the Platform Engineering Team.
B16	CC2.3 CC5.2	GupShup has configured the network devices and servers that are to be monitored for availability as per the Network Management procedure through the Zabbix network monitoring tool.
E15	CC5.2 CC5.3 CC6.1 CC6.3	Administrative access to the OCS Inventory tool is restricted to authorized personnel from the MIS Team.
E16	CC5.2 CC5.3 CC6.1 CC6.3	The administrative access to Freshdesk ticketing tool is restricted to authorized members from the Tech Support Team.
F21	CC6.1 CC6.2	**Granting of VPN Access to Datacenter Environment**

Control Reference	Mapped Criteria	Controls specified by GupShup
	CC6.3	The GupShup Team member raises a JIRA ticket to Infrastructure Operations team for provisioning Virtual Private Network (VPN) access to the third-party colocation datacenter and AWS environments which are reviewed and approved by GupShup Project Managers.
F22	CC6.1 CC6.2 CC6.3	**Revocation of VPN Access to Datacenter Environment** The users reporting Manager or MIS team basis on the requirement raises a Jira ticket to the infrastructure operations team for Revoking VPN access from Datacenter Environment.
F31	CC6.1 CC6.2 CC6.3	**Granting of user access to AWS** When a user requires access to the AWS, the user's reporting manager communicates the access request to the administrator by creating a JIRA ticket. Access is granted by Infrastructure Operations team to AWS based on the request from the user's manager.
F32	CC6.1 CC6.2 CC6.3	**Revocation of access from AWS** The users reporting Manager or MIS team basis on the requirement raises a Jira ticket to the infrastructure operations team for Revoking VPN access from AWS.
F33	CC6.1 CC6.2 CC6.3	Privileged and administrative access to the AWS is restricted to authorized personnel from the Infrastructure Operations team.

<table>
<tr><th>Control Reference</th><th>Mapped Criteria</th><th>Controls specified by GupShup</th></tr>
<tr><td>F23</td><td>CC6.1</td><td>GupShup has established an Asset Classification policy within the ISMS Policy. Asset inventory is currently maintained using the OCS Inventory tool.</td></tr>
<tr><td>E17</td><td>CC5.2
CC6.1
CC6.6</td><td>An encrypted site-to-site Virtual Private Network (VPN) tunnel has been established for enabling secure data transmission between GupShup Delivery Centers to the third-party colocation datacenter.</td></tr>
<tr><td>F25</td><td>CC6.1
A1.1</td><td>The SRE and Platform Team has established an internet facing Load Balancer for AWS Virtual Private Clouds (VPCs) in the production environment to manage the application load and restrict unauthorized access to VPCs.</td></tr>
<tr><td>F26</td><td>CC6.1</td><td>GupShup customers are hosted in a dedicated Virtual LAN (VLAN) within the third-party colocation datacenter/AWS VPC. Customers can access the hosted applications via a dedicated URL through Hypertext Transfer Protocol Secure (HTTPS) internet protocol.</td></tr>
<tr><td>F27</td><td>CC6.1
CC6.6</td><td>The FTP folders have been segregated for each GupShup customer by enabling access restrictions on the customer folders.</td></tr>
<tr><td colspan="3"><b>Complementary User Entity Control #4</b>
User organizations are responsible for ensuring that only authorized individuals have access to the FTP folders.</td></tr>
<tr><td>F28</td><td>CC6.1</td><td>Administrative activities performed on the servers within the third-party colocation datacenter are logged to monitor availability and performance of the servers.</td></tr>
</table>

Control Reference	Mapped Criteria	Controls specified by GupShup
D10	CC4.1 CC5.2 CC6.1 CC6.3	Administrative access on GupShup Domain Controllers is reviewed on a quarterly basis by the MIS Team.
F29	CC6.2 CC6.4	On a quarterly basis, the HR Team shares the deployment sheet capturing the active list of employees over email to the Facilities Team. The Admin & Facilities Team reconciles the deployment sheet against the active users with physical access to GupShup premises. In case of any discrepancies, the Admin & Facilities Team revokes the inappropriate access in a timely manner.
F30	CC6.1 CC6.2	On a quarterly basis, the HR Team shares the deployment sheet capturing the list of active employees over email to the MIS Team. The MIS Team reconciles the list of active employees against the list of active users from GupShup domain controller and shares the review acknowledgement / list of users with inappropriate access with the HR Team through email. In case of users with inappropriate access, the MIS Team revokes the credentials within the GupShup domain controller in a timely manner.

Common Criteria Related to System Operations

Control reference	Mapped Criteria	Controls specified by GupShup
Disaster Recovery		
G01	CC7.1 CC9.1	GupShup performs a Business Impact Analysis (BIA) as part of the IT Disaster Recovery Plan for GupShup's services and identifies potential threats that can impair system availability, and assess the risks associated with the identified threats on an annual basis.
E08	CC5.3 CC7.5 A1.3	Periodic tests (such as structured walkthroughs, simulation tests, emergency evacuation drills and tabletop session) are conducted at GupShup Delivery Centers in Mumbai, Bangalore, and Chennai. The tests include the following: Fortnightly, mock DR Drills are carried out to test the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The details of the test are documented on a JIRA Ticket, which is then reviewed and approved by VP, IT Annually, a tabletop/walkthrough test is performed by the Engineering Team and the results are reviewed and ap approved by VP, IT
F18	CC6.6 CC6.7 CC7.2 C1.1	GupShup has implemented Google Workspace Admin Data Loss Prevention (DLP) tool to monitor, detect and alert if any sensitive or confidential data is sent out of the GupShup network to external networks.

Control reference	Mapped Criteria	Controls specified by GupShup
		The DLP Security notification is shared across to the affected individuals via mail and a JIRA ticket is also logged for the security incident.
G02	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Security incidents reported by GupShup's employees/consultants and GupShup's customers are analyzed and resolved by the IT Security Team. The IT Security Team manually documents the security incident's occurrence date, severity, description, reported date, closure date, root cause, corrective action and status within a SIM Tracker. A JIRA ticket is logged for the reported security incident, the ticket is monitored and tracked to closure by the IT Security Team. If a GupShup's customer is impacted by the security incident, then GupShup informs/acknowledges to the customer within 2 hours of GupShup coming to know about the incident. A priority matrix is present for resolving the incidents on the basis of its severity. Resolution timelines are defined as per severity of the incident.
B09	CC2.3 CC7.2 CC7.3 CC7.4 CC7.5 CC2.3 CC6.5	GupShup has defined the process to report all the privacy, security related incidents and data breaches, in the 'Security Incident Management' document.

<table>
<tr><th>Control reference</th><th>Mapped Criteria</th><th>Controls specified by GupShup</th></tr>
<tr><td></td><td>C1.2</td><td></td></tr>
<tr><td colspan="3"><b>Complementary User Entity Control #5</b>
User organizations are responsible for reporting security incidents to GupShup via a dedicated email - "securitycompliance@GupShup.io".</td></tr>
<tr><td>G03</td><td>CC7.2
CC7.3
CC7.4</td><td>GupShup employees/consultants are provided awareness on security incident management and security incident reporting processes during the induction training conducted on the date of joining.</td></tr>
<tr><td>F19</td><td>CC6.6
CC6.8
CC7.1</td><td>GupShup has enabled Intrusion Prevention System (IPS) and web filtering system on the FortiGuard module within FortiGate Unified Threat Management (UTM) Tool to prevent any unauthorized access, breaches, and attacks.</td></tr>
<tr><td>D05</td><td>CC4.1
CC6.6
CC7.1
CC7.2</td><td>Corologix SIEM Tool is configured to monitor the corporate firewalls for the risks related to security, availability, and performance. The corporate firewalls have been configured to send security events to the Corologix SIEM Tool. The Platform Engineering Team monitors the event logs related to GupShup's corporate firewalls and performs the corrective actions in case of any noted observations.
GupShup performs a review of the rulesets enforced on the corporate firewall every quarter and corrective actions are taken in case of any noted deviations from the baseline.</td></tr>
<tr><td>B18</td><td>CC2.3
CC7.2
CC7.3</td><td>The GupShup customers are informed about the customer support channels during the customer on-boarding phase. GupShup customers seek help from the Tech Support Team by communicating via email to enterprise-support@GupShup.io or via telephonic support available on GupShup's website.</td></tr>
</table>

Control reference	Mapped Criteria	Controls specified by GupShup
	CC7.4	GupShup's key account customers seek help from the Tech Support Team by communicating via email to premiumcare@GupShup.io or via telephonic support available on GupShup's website. A Freshdesk ticket is raised by the Tech Support Team for queries /incidents reported by GupShup customers. Post providing resolution for the reported incidents/queries, the Freshdesk ticket is tracked to closure by the Tech Support Team.
F24	CC6.6 CC6.7 CC6.8 CC7.2 C1.1	Email attachments are scanned at the gateway to prevent infection from malicious software and programs using the Google Admin DLP. Relevant data protection rules are enabled through the Google Admin DLP to block the communication of Credit Card details, abuse words and PAN Card details within emails.
E18	CC5.2 CC7.3 CC7.5 A1.2	In case of a backup failure, an automated email notification is sent to Site Reliability Engineering/Platform Team regarding the backup failure. Based on the email notification, the SRE/ Platform Team logs a ticket in AWS Support Centre for backup failure resolution.
Complementary Subservice Organization Control #6 AWS is responsible for performing the corrective actions in case of backup failures, based on the request raised by SRE / Platform Team in AWS Support Centre.		

Common Criteria Related to Change Management

Control Reference	Mapped Criteria	Controls specified by GupShup
Change Management		
H01	CC8.1	**Change Authorization** Changes to be developed are communicated by the Product Team to the Engineering Team. The Product Team creates a request on JIRA and shares the change requirements with the Engineering Team. Change requirements include customer requested changes, application feature changes and enhancements identified by the Product Team.
Complementary User Entity Control #6 User organizations are responsible for communicating application changes or enhancements to GupShup.		
H02	CC8.1	**Change Development** Each request created by the Product Team is considered as a 'User Story' in JIRA. Each 'User Story' consists of multiple tasks and sub-tasks relating to customer requirements, application feature changes and enhancements. The developers make a copy of the Master Production trunk (the section after the last release went live) from the code repository tool, GitLab on their individual systems. This copy is referred to as the Develop branch.

Control Reference	Mapped Criteria	Controls specified by GupShup
H02	CC8.1	**Change Development** Each request created by the Product Team is considered as a 'User Story' in JIRA. Each 'User Story' consists of multiple tasks and sub-tasks relating to customer requirements, application feature changes and enhancements. The developers make a copy of the Master Production trunk (the section after the last release went live) from the code repository tool, GitLab on their individual systems. This copy is referred to as the Develop branch.
H03	CC8.1	**Code Review** The developer raises a Pull Request on the code repository tool, GitLab once the development is complete indicating that the code is ready for review before being tested by the QA Team. The developer selects the reviewers on the code repository tool, GitLab who get an email notification that the developed code is ready for their review. Reviewers review the code and provide comments against the modified/updated code if necessary. Developers make modifications to the code if required based on the review and then re-submit the code changes on the Pull Request. Upon reviewing the modifications to the code, the reviewer approves and merges the code.

Control Reference	Mapped Criteria	Controls specified by GupShup
H04	CC8.1	**Change Testing - Feature Testing** Feature Test cases are defined by the developers at the beginning of the sprint cycle. Code that has been reviewed is ready for testing. Feature testing of the developed code is performed by the developers on their systems.
H05	CC8.1	**Change Testing - Security Testing** Once Feature testing is successfully completed, the QA Team performs a manual security testing of the developed code in the QA environment. After successful completion of Security testing, the QA Team provides sign-off for moving the code to the Vulnerability testing stage.
H06	CC8.1	**Change Testing - Vulnerability Testing** The vulnerabilities identified, if any are documented through a JIRA ticket and necessary corrective actions are performed by the Operations Team. Code related vulnerabilities are addressed by the Engineering & DevOps Team. A sign-off is provided by the QA Team in case of successful testing or comments in case of issues noted.

Control Reference	Mapped Criteria	Controls specified by GupShup
		Sign offs are also provided by the Tech Support, General Support, and the Product Manager. Additionally, Operations Team provides sign off in case of DB Changes.
H07	CC8.1	**Change Testing – UAT** User Acceptance Testing (UAT) is only carried out for customer requested changes and hence are not mandatory for the internal changes. When the Product Team determines that a UAT is required, it is performed by the Product Manager in the UAT environment and the sign-off is provided via email.
H08	CC8.1	**Change Deployment in Production** Based on code merged, multiple jobs are automatically triggered on the Jenkins tool to deploy the code in production environment. The deployment is monitored for any failures and appropriate actions are taken.
H09	CC8.1	**Segregation of Environment** GupShup has established different environments for development, QA, UAT and production and has established controls to ensure segregation of production data from the development and QA environments.

Control Reference	Mapped Criteria	Controls specified by GupShup
E03	CC5.1 CC8.1	**Segregation of Duties** Segregation of duties has been enforced to ensure that only the Development Team has access to check out code for development and only the Senior Team member from the Engineering & DevOps Team have access to deploy the code into Production.
H10	CC8.1	The Tech Support Team raises a JIRA ticket mentioning the change management request and assigns the ticket to the Engineering / Product Management teams. The JIRA ticket raised by the GupShup Tech Support Team will be closed post obtaining the custom developments resolution from the Engineering/Product Management teams.
H11	CC8.1	GupShup has defined the change management process within the Change Management document, to ensure that changes are assessed, approved, tested and implemented in a controlled manner. The Change Management document is uploaded onto the Google drive for reference of all GupShup employees.

Common Criteria Related to Risk Mitigation

Control Reference	Mapped Criteria	Controls specified by GupShup
Risk Mitigation Strategy		
C02	CC3.2 CC3.3 CC5.1 CC5.3 CC9.1	The IT Security Team prepares a risk treatment plan based on risk ratings/ net risk value which is documented in Risk Register and Residual Risk is calculated. The Residual Risk is reviewed and accepted by the Risk Owner based on the defined timeline.
C06	CC3.2 CC4.1 CC5.1 CC5.2 CC9.2	**Monitoring of Commitments – Infrastructure Service Providers** GupShup obtains SOC Attestation reports from its third-party colocation datacenter and cloud service provider on an annual basis and verifies that the risks associated to the services obtained are addressed adequately with controls and processes implemented by the third-party datacenter vendors.
Complementary Subservice Organization Control #7 Third party datacenters are responsible for providing representations and security assurances about the controls at their datacenters on a periodic basis.		

Additional Criteria for Availability

Control Reference	Mapped Criteria	Controls specified by GupShup
Environmental Controls		
J01	A1.2	Smoke detectors, fire alarms and fire extinguishers are installed at strategic locations and the server room within the GupShup premises.
Complementary Subservice Organization Control #8 Subservice organizations are responsible for maintaining adequate environmental safeguards to their datacenter locations, as follows: Implementing fire extinguishers, smoke detectors, UPS, temperature & humidity control		
J02	A1.2	Preventive maintenance for smoke detectors, fire alarms, fire extinguishers, and fire suppression systems are performed on a yearly basis.
Complementary Subservice Organization Control #9 Subservice organizations are responsible for maintaining adequate environmental safeguards to their datacenter locations, as follows: Carrying out preventive maintenance of the above equipment's on a periodic basis.		
J03	A1.2	Power backup for the GupShup premises, including the server room is provided through Uninterrupted Power Supply (UPS) systems. Preventive maintenance is performed on a yearly basis, for the UPS systems.
Complementary Subservice Organization Control #10		

Control Reference	Mapped Criteria	Controls specified by GupShup
Subservice organizations are responsible for maintaining the equipment and infrastructure required for managing and maintaining the Power Supply systems and generators for uninterrupted power supply.		
J04	A1.2	Air-conditioners are installed inside the server room to control and maintain the temperature and humidity conditions.
Complementary Subservice Organization Control #11 Subservice organizations are responsible for installing and maintaining air-conditioners inside the datacenters. The subservice organizations are also responsible for monitoring the temperature and humidity conditions on a periodic basis.		
Backup and Restoration		
E11	CC5.2 A1.2	**Third Party Datacenter – Database Backup and Replication** A daily automated backup of all the databases in the production environments hosted in the third-party colocation datacenters is carried out using Xtrabackup tool.
E12	CC5.2 A1.2	**AWS Relational Database Backup** An automated weekly full backup is performed on the AWS Relational Database Services (RDS) instances and the backup logs are retained for a period of 7 days.

Control Reference	Mapped Criteria	Controls specified by GupShup
G04	CC7.5 A1.2 A1.3	Restoration testing of backups on AWS and third-party colocation datacenters is performed on a quarterly basis by the Infrastructure Operations team and the results are documented on a JIRA ticket.
E19	CC5.2 A1.2	**AWS AMI Instance Backup** The Amazon Machine Images (AMI) instance backups are performed on a daily basis using the policies configured in Amazon Data Lifecycle Manager. The Amazon Machine Image (AMI) instance backups are retained for a period of 7 days.
J05	A1.1 A1.2	GupShup has defined service uptime SLAs within the Master Service Agreement (MSA) signed with its customers and monitors and reports it on a continuous basis.

Additional Criteria for Confidentiality

Control Reference	Mapped Criteria	Controls specified by GupShup
Confidentiality Agreements		
A04	CC1.1	On the day of joining, the employees are required to sign GupShup's Non-Disclosure Agreement (NDA) which includes clauses for confidentiality, exclusive employment, period of effectiveness and breach of confidentiality.
B04	CC2.2 CC2.3 CC5.3 C1.1	GupShup has defined a Non-Disclosure Agreement (NDA) documenting the confidentiality requirements and clauses relating to non-disclosure and data protection for the services provided by the third-party colocation datacenter and cloud service provider. The NDA is signed by the relevant stakeholders from GupShup and third-party colocation datacenters and cloud service provider.
Complementary Subservice Organization Control #12 The third-party colocation datacenter and cloud service providers are responsible to ensure the commitments to confidentiality as per the agreed NDA signed with GupShup.		
Protection of Customer Data		
B14	CC2.2 CC5.3 C1.1 C1.2	**Handling of Customer Data** GupShup as part of its Data Classification and Handling Policy has established procedures for handling the information shared by customers including its retention and disposal.

Control Reference	Mapped Criteria	Controls specified by GupShup
B20	CC2.3 CC6.5 C1.2	GupShup has established a process to destroy/erase/anonymize personal information records as specified in the Data Retention and Disposal policy using appropriate data destruction techniques. Post the data retention period, destruction of relevant company data using appropriate data destruction techniques is carried out basis the existing statutory norms. A JIRA ticket is also raised which captures the data being destroyed/erased/anonymized.
B21	CC2.3 CC6.5 C1.3	GupShup has established a shredding process to dispose the physical hard copy data such as paper output containing personal information using the paper shredder.
Complementary Subservice Organization Control #13 The third-party vendors are responsible to ensure that post the data retention period, the data is destroyed using appropriate data destruction techniques and the deletion certificate is shared with GupShup.		
H12	CC8.1 C1.1	Confidential data transferred within the production environment is encrypted using Java AES-256 Encryption.
K01	C1.1	Data stored in the production databases and S3 buckets are encrypted.

Appendix A – Complementary User Entity Controls

CUEC Reference	CUEC Description	Control Reference
CUEC #1	User organizations are responsible for communicating changes to the MSA and for reviewing and signing-off on the changes.	B03
CUEC #2	User organization is responsible for communicating the incident/query to GupShup via email and for confirmation of the resolution of incident/query.	B15
CUEC #3	User organizations are responsible for reviewing the customer reports containing details of service requests, incidents, change request and problem management cases.	B17
CUEC #4	User organizations are responsible for ensuring that only authorized individuals have access to the FTP folders.	F27
CUEC #5	User organizations are responsible for reporting security incidents to GupShup via a dedicated email - "securitycompliance@GupShup.io".	G02
CUEC #6	User organizations are responsible for communicating application changes or enhancements to GupShup.	H01

Appendix B – Complementary Subservice Organization Controls

CSOC Reference	CSOC Description	Control Reference
CSOC #1	The vendors are responsible to ensure the commitments to integrity and ethical values are upheld as per the agreements signed with GupShup.	A10
CSOC #2	Subservice organizations are responsible for restricting the physical access to their premises to authorized personnel.	F03
CSOC #3	Subservice organizations are responsible for monitoring their physical premises through CCTV cameras.	F05
CSOC #4	Subservice organizations are responsible for restricting the physical access to the server rooms to authorized personnel.	F06
CSOC #5	Third party colocation datacenter and cloud service provider are responsible for performing the hardening procedures for their network devices.	D08
CSOC #6	AWS is responsible for performing the corrective actions in case of backup failures, based on the request raised by SRE / Platform Team in AWS Support Centre.	E18
CSOC #7	Third party datacenter and cloud service provider are responsible for providing representations and security assurances about the controls at their datacenters on a periodic basis.	C06

CSOC #8	Subservice organizations are responsible for maintaining adequate environmental safeguards to their datacenter locations, as follows: Implementing fire extinguishers, smoke detectors, UPS, temperature & humidity control	J01
CSOC #9	Subservice organizations are responsible for maintaining adequate environmental safeguards to their datacenter locations, as follows: Carrying out preventive maintenance of the above equipment's on a periodic basis.	J02
CSOC #10	Subservice organizations are responsible for maintaining the equipment and infrastructure required for managing and maintaining the Power Supply systems and generators for uninterrupted power supply.	J03
CSOC #11	Subservice organizations are responsible for installing and maintaining air-conditioners inside the datacenters. The subservice organizations are also responsible for monitoring the temperature and humidity conditions on a periodic basis.	J04
CSOC #12	The third-party colocation datacenter and cloud service providers are responsible to ensure the commitments to confidentiality as per the agreed NDA signed with GupShup.	B04
CSOC #13	The third-party vendors are responsible to ensure that post the data retention period, the data is destroyed using appropriate data destruction techniques and the deletion certificate is shared with GupShup.	B21