Bizzdesign

SOC 3 Report

Report about Bizzdesign Alfabet Cloud Service relevant for **Security** and **Availability**

Period February 1st, 2025 to May 31st, 2025

Organization	Bizzdesign
System	Bizzdesign Alfabet Cloud Service
Type of Report	SOC 3
Reporting Period	February 1st, 2025 to May 31st, 2025
Description	SOC 3 Report about Bizzdesign Alfabet Cloud Service relevant for Security and Availability
Date of Report	September 8, 2025
Reference	Bizzdesign-Alfabet-2025-SOC3

Contents

SECTION I – Management Assertion of Bizzdesign Alfabet Cloud Service

To whom it may concern

Enschede, September 8, 2025

Subject: Management Assertion of Bizzdesign

We are responsible for designing, implementing, operating, and maintaining effective controls within Bizzdesign Alfabet Cloud Service (system) throughout the period February 1st, 2025 to May 31st, 2025, to provide reasonable assurance that Bizzdesign's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1st, 2025 to May 31st, 2025, to provide reasonable assurance that Bizzdesign's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Bizzdesign's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We use subservice organizations AWS and Microsoft to provide infrastructure and services that underpin parts of the system. The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only

be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of Bizzdesign Alfabet Cloud Service also indicates the complementary subservice organization controls assumed in the design of Bizzdesign's controls. The description does not disclose the actual controls at the subservice organization.

The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Bizzdesign's controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents the complementary user entity controls assumed in the design of Bizzdesign's controls.

We assert that the controls within the system were effective throughout the period February 1st, 2025 to May 31st, 2025, to provide reasonable assurance that Bizzdesign's service commitments and system requirements were achieved based on the applicable trust services criteria.

Peter Matthijssen

CPO

Bizzdesign

08-09-2025

SECTION II – Independent Service Auditors' Assurance Report

2-Control B.V.
Haagsemarkt 1
4813 BA Breda
The Netherlands

+31 (0)76 50 194 70
www.2-control.nl
info@2-control.nl

To management of Bizzdesign
Capitool 15
7521 PL Enschede
The Netherlands

Breda, September 8, 2025

Reference: 2C-2025-771

Below you find our Independent Service Auditors' Assurance Report for ISAE 3000 / Service Organization Control 3 statement.

Opinion
In our opinion, management's assertion that the controls within Bizzdesign Alfabet Cloud Service were effective throughout the period February 1st, 2025 to May 31st, 2025, to provide reasonable assurance that Bizzdesign's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Scope
We have examined Bizzdesign's accompanying assertion titled "Management Assertion of Bizzdesign Alfabet Cloud Service" (assertion) that the controls within Bizzdesign Alfabet Cloud Service (system) were effective throughout the period February 1st, 2025 to May 31st, 2025, to provide reasonable assurance that Bizzdesign's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with revised points of focus - 2022), in AICPA, Trust Services Criteria.

Sub-service organizations
Bizzdesign uses subservice organizations AWS and Microsoft to provide infrastructure and services that underpin parts of the system. The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of Bizzdesign Alfabet Cloud Service also indicates the complementary subservice organization controls assumed in the design of Bizzdesign's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Objectives at the user entity (Complementary User Entity Controls)
The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Bizzdesign's controls are suitably designed and operating effectively, along with related controls at the service organizations. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Restricted use
This report and the description of tests of controls and results thereof are intended solely for the information and use of Bizzdesign user entities of Bizzdesign Alfabet Cloud Service during some or all of the period February 1st, 2025 to May 31st, 2025 and 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

2-Control B.V.
Haagsemarkt 1
4813 BA Breda
The Netherlands

+31 (0)76 50 194 70
www.2-control.nl
info@2-control.nl

- How the service organization's system interacts with user entities, subservice organization, and other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria 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.

Service organization's responsibilities
Bizzdesign 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 Bizzdesign's service commitments and system requirements were achieved. Bizzdesign has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Bizzdesign is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditor's responsibilities
Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA – RKBN), and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Bizzdesign's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Bizzdesign's service commitments and system requirements based the applicable trust services criteria.

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

2-Control B.V.
Haagsemarkt 1
4813 BA Breda
The Netherlands

+31 (0)76 50 194 70
www.2-control.nl
info@2-control.nl

Inherent limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Drs. Ing. A.P.J. Mouwen RE CISA

08-09-2025

2-Control B.V.
Haagsemarkt 1
4813 BA Breda

Attachment A – Description of Bizzdesign Alfabet Cloud Service

Description

Services

The scope of this report covers all critical systems, applications, networks, human resources, and information assets directly connected with the provisioning and operation of the Bizzdesign Alfabet Cloud Service services Bizzdesign offers to customers.

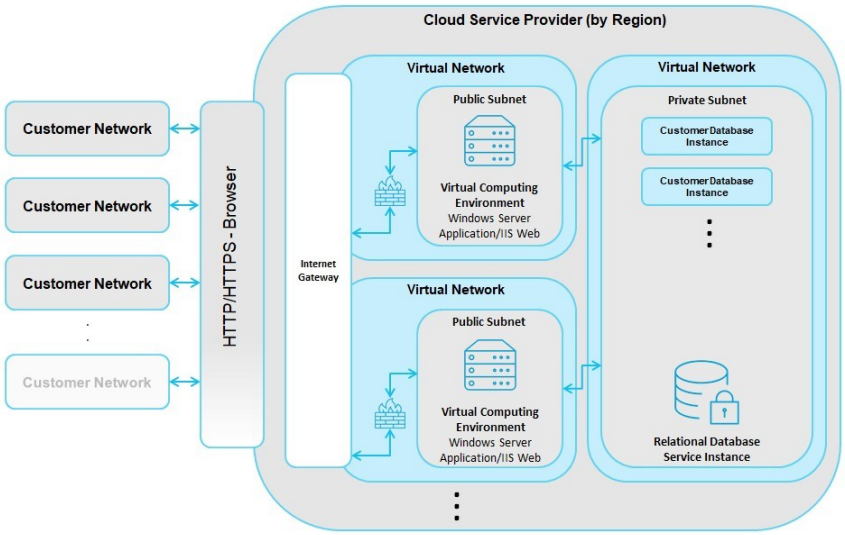
Alfabet FastLane

Alfabet FastLane is the latest SaaS solution for IT Portfolio Management from Bizzdesign. The solution enables customers to navigate the complexity of IT portfolio management by turning unanswered questions into meaningful business insights. Alfabet FastLane is a pre-configured cloud product, which is the simplest Information Technology Portfolio Management (ITPM) solution in terms of usability and understanding from Bizzdesign. Alfabet FastLane allows customers to carry out enhanced decision-making, drive innovation, and reduce time-to-market for portfolio planning. It creates operational efficiencies by eliminating information silos within organizations – thereby improving compliance to standard practices and reduces business and technical risk associated with IT Portfolio Management.

Alfabet FastLane leverages the experience of Bizzdesign in providing market leading Enterprise Architecture (EA) and ITPM solutions for over two decades. In order to help ensure that customer portfolio maturity evolves over time, the Alfabet FastLane offering can be migrated to Alfabet Enterprise with ease, requiring minimal effort and time. The solution offers guided portfolio data entry, a feature that allows customers to reduce the total cost of ownership and removes the common barriers that low-maturity customers face when setting up their IT portfolio. Alfabet FastLane is a low-cost and low-risk ITPM solution, one that allows customers to achieve organizational agility while streamlining their IT processes and gaining improved decision-making ability.

Alfabet FastLane customer instances are hosted on dedicated virtual machine instances with a multi-tenant relational database service instance hosting a database instance for each customer.

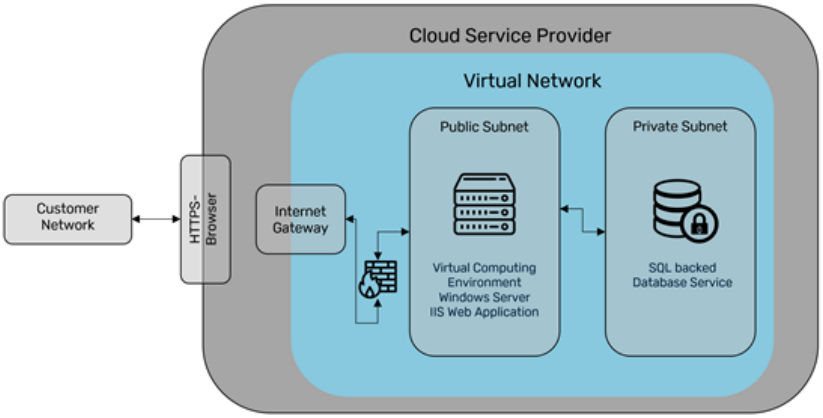
Logical Deployment Architecture



Alfabet Cloud Enterprise

Alfabet Cloud Enterprise is a dedicated SaaS solution using a single-tenant concept where customers dedicate resources encapsulated in a Virtual Network. Customers can select between several different geographical regions for hosting their tenant depending on best connectivity.

Logical Deployment Architecture



In some deployment scenarios customers can use Bizzdesign Alfabet Cloud Service services outside of the SaaS solution; for those scenarios this report is not applicable.

This report covers Bizzdesign's Alfabet SaaS services offered from the following AWS and Azure data centers:

Fastlane	Enterprise
AWS - Asia Pacific (Sydney)	AWS - Asia Pacific (Sydney)
AWS - US East (Northern Virginia)	AWS - Asia Pacific (Singapore)
AWS - Europe (Frankfurt)	AWS - US East (Northern Virginia)
	AWS - US West (Northern California)
	AWS - US West (Oregon)
	AWS - South America (São Paulo)
	AWS - Canada (Central)
	AWS - Europe (London)
	AWS - Europe (Paris)
	AWS - Europe (Ireland)
	AWS - Europe (Frankfurt)
	AWS - East US (Virginia)
	AZURE - West US (Washington)
	AZURE - Central US (Iowa)
	AZURE - South Central US (Texas)
	AZURE - East US (Virginia)
	AZURE - Brazil South (São Paulo)
	AZURE - Canada Central (Toronto)
	AZURE - UK South (London)
	AZURE - North Europe (Ireland)
	AZURE - Germany West Central
	AZURE - West Europe (Netherlands)
	AZURE - Australia East (New South
	AZURE – Qatar
	AZURE - Central India
	AZURE - South Africa North
	AZURE - UAE North (Dubai)

System Components

The following system components are part of the services as provided by Bizzdesign;

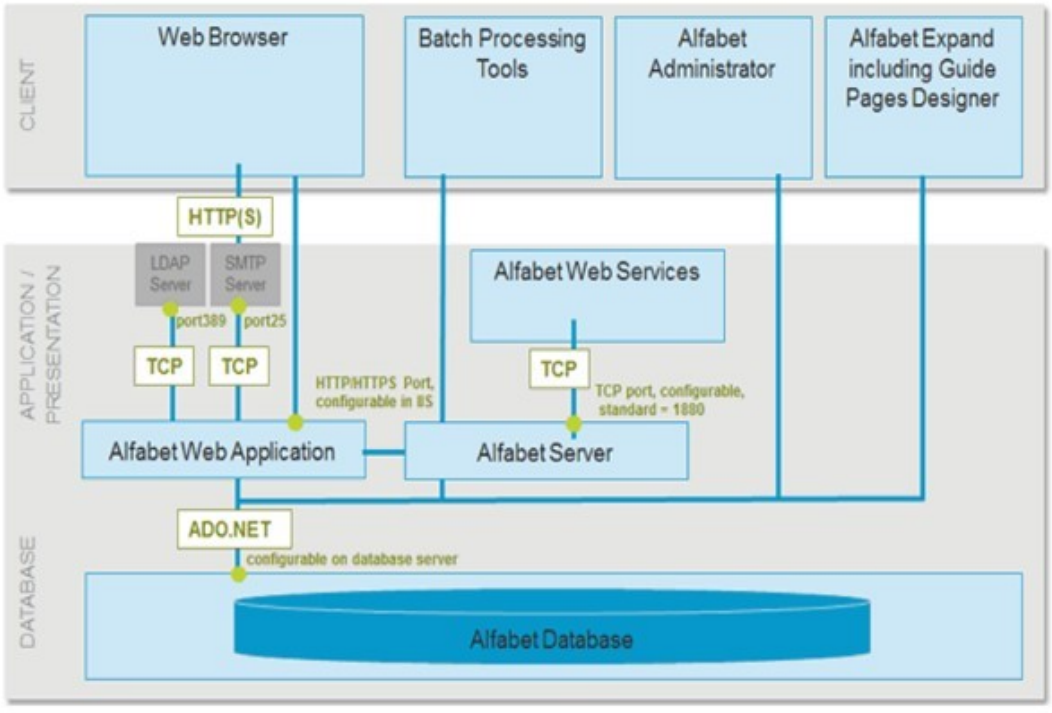
a. Infrastructure-as-a-Service (IAAS) Provider Infrastructure services

The system is primarily hosted either on Amazon Web Services (AWS) or Azure infrastructure. The supporting systems (e.g. monitoring services) supporting the delivery of Cloud services are described further on in this document.

b. Software

Bizzdesign applications part of the system

Alfabet customer instances are hosted on dedicated virtual machine instances with a relational database service instance hosting a database instance for each customer. The Alfabet service consists of a .NET/C# application server running on Windows computers that allows users to access the application server using a web browser.



Alfabet Cloud Service Software

• Windows Operating System: Alfabet Cloud server instances are running Windows Operating system and are licensed through IaaS Virtual Computing service.

• Microsoft SQL Database: Microsoft SQL Server® is a relational database management system developed by Microsoft. It is used to store and manage Alfabet data.

• Password manager: lets the companies centrally manage, administer, and share passwords and access data and documents. You decide down to the smallest detail what access rights a user is granted, what folders or entries can be viewed, or for example, what kind of activities should be tracked.

• Identity and Access Federation: The Security Assertion Markup Language (SAML) component is fully compliant with the OASIS Security Assertion Markup Language v2.0 specification.

See http://www.componentspace.com/SAMLv20.aspx

• UsingIT: Tool used for documentation of Application configuration changes by internal supplier Alfabet TechConsulting. It is based on the Alfabet software developed and implemented by the Alfabet TechConsulting Team.

Third-party software

Various third-party software components are used to provide the system, the core third party components are:

- A relational database system
- A web server
  Identity and Access Federation: The Security Assertion Markup Language (SAML)
  See http://www.componentspace.com/SAMLv20.aspx
- .NET Framework

The above platform architecture provides some additional information on how the different components interact with each other, and how the solution operates.

Full SaaS Platform Architecture: Other important software used in provisioning and maintenance of the system

Several software applications are used to create and manage the system. The most important component is Azure DevOps, a system used to track both development tasks, security issues, status of ISMS controls/exceptions and change requests. As such this component is in scope for this report.

c. People

Management Team

The management team is overall responsible for the decision making within Bizzdesign. The management team is composed of experienced executives, with a broad and diverse range of technology, financial, sales and general business experience. The management team plays a critical role in the operations of the company. The management team meets on a regular basis to discuss operations matters for quick decision making and implementation, and general strategy aspects of the business. The management team communicates with the operational level management.

Information Security Group

The information security group defines high-level security objectives and approves security policies, and is ultimately responsible for security governance, training and awareness, product and platform security and security operations.

R&D & Cloud Service Operations

The R&D and Cloud Service Operations team is led by the Chief Product Officer (CPO) and is broadly divided into two teams: R&D and Cloud Service Operations.

The R&D team is responsible for delivery of the product roadmap, secure and stable applications, and bug resolution.

The Cloud Service Operations team is responsible for the architecture of the services which exist across the AWS and Azure environment and for the design and implementation of adequate and appropriate measures for ensuring that availability and security requirements are met. The team is also responsible for supporting the production environment, monitoring for issues and events, and incident and change management for the SaaS environment.

Support Team

The support team is led by the Chief Customer Officer and is responsible for providing support to customers. The support team interacts with customers and plays an important role in discussing issues, features requests and other input from customers with the development team.

Sales, Consultancy and Marketing

The sales, consultancy and marketing functions are organized into the geographical segments in which they operate. These divisions spearhead the marketing, sales and consultancy initiatives and are responsible for positioning Bizzdesign's services in the global market.

Finance and Legal

The Finance and Legal team is responsible for meeting financial reporting compliance requirements, as well as corporate compliance and risk management, and is led by the Chief Financial Officer (CFO).

Human Resources

The human resource team is led by the Chief Human Resources Officer (CHRO) and is ultimately responsible for identifying, on-boarding and retaining suitably qualified team members, overseeing ongoing training and education requirements and off-boarding of terminated personnel.

d. Procedures

Bizzdesign has several procedures relevant for achieving the stated service commitments:

Procedure	Description
Authorization	This defines how employees are granted access to various systems. This includes checks to ensure proper separation of duties is maintained and is based on a "principle of least privilege"; employees are only authorized to access systems when needed to perform their duties.
Change Management	This defines the process followed when implementing changes to IT systems and includes steps to safeguard against data loss and unavailability of applications.
Disaster Recovery	This describes what steps to perform in case of a large outage affecting multiple customers.
HR Onboarding and Offboarding	These ensure new employees are screened, receive proper training and have knowledge of company policies and procedures. When offboarding special attention is given to blocking accounts, returning of company assets and reminding employees about confidentiality agreements.
Incident Management	This procedure provides guidelines in case an incident occurs. The procedure aims to identify the cause and scope of any potential security breaches and other incidents as fast as possible, limit the scope of any security breaches and then return all services to operational status swiftly and effectively.

Procedure	Description
Operational Management	This describes policies and procedures for performing patch- and vulnerability management, operational monitoring and follow-up to monitoring alerts and backup and recovery procedures.
Risk Assessment and Mitigation	The aim of this procedure is to periodically identify and mitigate risks that might impact the system.
Security Management	This describes how various security aspects are monitored, and in which way alerts that are triggered should be analyzed and resolved.
Software Development Lifecycle	This contains the process and procedures used for software development. The goal of the Software Development Lifecycle is to increase software quality, both in terms of availability and security, by implementing a standardized process based on industry best practices.
Support Access	This describes how Bizzdesign support can access customer data, including the ways in which a customer can grant that access.

e. Data

The following types of data are stored in the system:

- Configuration settings for the various components of the system, stored in files and a database system.
- Information about users of the system, representing their assigned privileges, name, e-mail address, login name and in some cases an encrypted password, which is stored in a database system.
- Data generated by the users of the system through use of the Bizzdesign applications, which is stored in database systems. Bizzdesign has no control over what types of data are stored in the system by the users.

In addition to the data in the system customers can submit support requests through our support desk application.

f. Boundaries

This report only covers the provisioning and operation of the system. Other aspects such as billing/invoicing and consulting services are not included in the scope of the report.

This report does not cover third-party applications and/or platforms that interact with the system using API.

g. Third-party Access

The software and systems described in the paragraph “System Components” are partially maintained by third parties. These third parties are subject to our Third-Party IT Services Policy which contains safeguards regarding security and confidentiality of data potentially accessible by these third parties.

System Incident

During the audit period the system has experienced no significant incidents that were either related to ineffective controls or otherwise (could have) resulted in problems meeting service commitments.

Trust Service Criteria and Controls

The common criteria are organized into categories as described as follows.

Organization and Management

Bizzdesign Organization & Management

Bizzdesign’s organizational structure provides the framework within which its activities for achieving entity wide objectives are planned, executed, controlled, and monitored. The organization has established documented procedures to ensure those criteria relevant to how the organization is structured and the process that organization has implemented to manage and support people within its operating unit, are satisfied. Bizzdesign operates under the general direction of its senior management which is also responsible for the day to day management. Job descriptions are in place and define roles and responsibilities, skills and knowledge requirements. Bizzdesign’s organizational structure, reporting relationships, authorities and responsibilities are evaluated and reviewed at least annually by the management team. Once approved, changes are communicated to employees if applicable.

Bizzdesign overall Security

Bizzdesign has developed an organization wide Information Security Management Framework aligned with the ISO/IEC 27000 family of security standards. Included in the framework are policies, standards and procedural documentation relating to security and confidentiality of information and information systems. The Global IT & Security Manager has overall responsibility for Bizzdesign’s security framework. The Global IT & Security Manager reports to a senior member of the management team. Information Security is a standing item

on the agenda of the management meetings, which includes security initiatives, projects, reviewing open items and discussions around current and emerging threats occurring in the industry if applicable. The Global IT & Security Manager is responsible for reviewing Bizzdesign's Information Security Policy on an annual basis, and for aligning the changes in policy to new business and technology requirements as they are identified. Changes to any of Bizzdesign's policies and standards, including the Information Security Policy, are reviewed and approved by the Information Security Group (ISG).

Human Resources

Human Resources (HR) policies form part of the IT policies and describe security measures that Bizzdesign has in place for the HR function. The HR team defines policies and procedures for recruitment, onboarding and termination of employment. The policies define terms and conditions of employment, requirements for information security awareness, education and training, termination or change of employment and pre-employment checks. All policies, standards and procedures are documented and made available to personnel through Bizzdesign's SharePoint environment.

Bizzdesign's HR department is responsible for the following actions as part of the life cycle of an employee:

- The HR team performs background screening and verification checks for the candidate as part of the onboarding procedure. The background checks are used to assess a candidate's education, training / qualifications, previous employment and experience as well as relevant criminal records. These checks are carried out in accordance with applicable local laws.
- The employee is required to sign an employment agreement with the company which includes clauses for maintaining confidentiality and non-disclosure of information.
- The employee must read and acknowledge their understanding of Bizzdesign's IT (security) policies and employee handbook.
- Following termination of employment (either by Bizzdesign or the employee), the HR Team works with IT and the employee's manager to ensure a separation checklist is followed and all tasks completed.

Communication

Internal Communication

Bizzdesign maintains communication with personnel using internal collaboration tools, e-mail, calls and for instance annual kick-off events. The communication includes, but is not limited to, communication of Bizzdesign's policies and procedures, corporate events, new initiatives,

and security awareness. Changes and updates to Bizzdesign policies and procedures, and implementation of changes on Bizzdesign network and security devices are communicated to relevant Bizzdesign personnel through internal collaboration tools.

External Communication

Bizzdesign utilizes agreements, its website and email to communicate to external customers, vendors, and other parties. Customers have access to the support portal, this portal is used to provide information about the product and to log, and follow up, on support tickets. Customers are also assigned to Account Executives from Bizzdesign. Service Level Agreements, this SOC2 report and customer contracts, clearly communicate to customers the functionality of the services provided, and the responsibilities of each party in relation to such services (this includes information on the boundaries that exist between Bizzdesign's provision of the services, and a customer's use of the services).

Risk management and design and implementation of controls

Risk Identification

Bizzdesign generates information on information security risks from the following sources:

- Risk and threat modelling by the ISG.
- Risk and threat modelling by internal business and software development teams during the development of new or updated product features.
- Annual penetration testing by third party specialists and regular vulnerability assessments of the application.
- Operational data and alerts from application and infrastructure log analysis.
- Ongoing monitoring of compliance activities and trends.
- Subscription to relevant newsletters and attendance at relevant forums.

Information security risks are managed through several processes:

- Application-level controls for risks that have been identified by risk and threat modelling, results of penetration or vulnerability testing are managed using the normal development lifecycle workflow management and tracking tools, with defined fast track processes for high-risk vulnerabilities or bugs in production systems.
- Infrastructure risks, including infrastructure patching and configuration, are managed as an integral part of operational management processes by the Cloud Service Operations team, who are also responsible for infrastructure security monitoring.

- Application security monitoring, including anomalous application behavior detection and response, is managed by the Cloud Service Operations team.

Risk Management

Oversight of information security risk at a corporate level is undertaken by the ISG. The ISG consists of several senior C-level executives with different backgrounds. Information security is a standing item on the agenda of the management team, and the ISG considers key risks for which high level governance and management decisions are required. Bizzdesign has a formalized risk management process and maintains a list of risks in the ISMS which tracks key risks to the organization, including information security risks. Risk assessments include a review of internal and external factors that threaten the achievement of business objectives. Mitigating controls are identified for all risks and risks with residual scores above the acceptable risk threshold have mitigating actions agreed that are then tracked by the ISG.

Controls Overview

Bizzdesign has developed formal company-wide policies and procedures for meeting the requirements related to security. Policies are available via the company intranet to all personnel. The Information Security Policy includes:

- Acceptable Use Policy
- Access Control Policy
- Backup Policy
- Change Management Policy
- Clear desk and Screen Policy
- Cryptography Policy
- Incident Response Plan
- Information Classification and Treatment Policy
- Password Policy
- Physical Protection Policy
- Risk Assessment and Treatment Mitigation Methodology
- Software Development Lifecyle Policy
- Third-Party Management Policy

Separate policies and procedures are defined for Business Continuity and Disaster Recovery, which are tested on a periodic basis. All policies are kept up to date and reviewed on an annual basis, or more frequently as necessary (for example, based on an updated risk assessment).

Monitoring of Controls

Security

An incident response process is in place to document incidents and work on resolutions. A root cause analysis may also be performed on security incidents if deemed necessary. For high severity security incidents, regular status update meetings are held to discuss and monitor the status. The Global IT & Security Manager conducts at least quarterly compliance checks against the security policy and access control standards. This includes checks that quarterly user access reviews are performed for production systems and network access. Password settings for systems are also included in the review. On an annual basis the Global IT & Security Manager completes supplier reviews. This includes receiving compliance reporting from subservice organizations (i.e. SOC 2 reporting for AWS and Azure) and reviewing the reports for any issues. Should any issues be identified, they will be logged and assessed to determine the impact on the Bizzdesign environment. The Global IT & Security Manager performs an annual internal audit to review the design and operating effectiveness of internal controls. The results of these reviews are reported to the ISG with response plans developed in relation to material deficiencies if deemed necessary.

Ongoing Monitoring

Automated Monitoring Systems: Bizzdesign uses a wide variety of automated monitoring systems, which cover security, service performance and availability. Monitoring tools are implemented to detect and protect against external and internal threats. System performance including availability is also continuously monitored through a specific set of tools and control procedures.

Client Services: A dedicated support team is in place to service customer requests and monitor customer feedback for performance. If recurring performance issues are reported by customers, the support team will create an internal issue for the Cloud Service Operations team to investigate. External customers communicate with the service desk through the support portal, and an 24x7 phone line is available for reporting critical (performance) issues that have a major impact on customer's operations.

Complementary Customer Control Considerations and User Entity Responsibilities

The System offered by Bizzdesign is operated under a shared responsibility model. Bizzdesign is responsible for maintaining security and availability of the System components under its control, but the Customer using the System has certain responsibilities as well.

Availability

Internet Access

The System is accessed over the internet. The Customer is responsible for maintaining an internet connection that meets the system requirements specified by Bizzdesign.

Preventing unauthorized access

Bizzdesign supplies the Customer with a single administrator account for the System. The Customer is responsible for:

- Setting the initial password for this account.
- Creating and removing user accounts within the System (either manually or by using a Single Sign On solution linking to the Customer's authentication system).
- Assigning privileges to those user accounts with the appropriate access rights.
- Regularly reviewing the list of user accounts and associated access rights.
- Configuring account security policies such as multi-factor authentication and password expiration and security requirements within the System or the linked Single Sign On solution.
- All other aspects related to user management and privilege assignment.
- Security of devices and software used to access the System.

Encryption of data in transit and at rest

Bizzdesign configures the System in such a way that connections to the System are only allowed using encrypted connections conforming to industry-standard best practices to secure data in transit between the System and the Customer. Data stored in the system will be encrypted in line with industry-standard best practices to secure data. Once data leaves the System responsibility for encryption (both at rest and while transferring between the Customer's systems) passes to the Customer.

Virus and malware scans

Data uploaded to the System by the Customer should be scanned for viruses and other malware by the Customer both before uploading, and when downloading it from the System; due to the way data is stored and encrypted Bizzdesign is not always able to scan this data.

Controls at Subservice Organizations

Bizzdesign uses AWS and Microsoft as a subservice organization to provide infrastructure and services that underpin parts of the System. For many of the Trust Services Criteria the related controls are managed and monitored by Bizzdesign under the AWS and Microsoft shared responsibility model. (https://aws.amazon.com/compliance/shared-responsibility-model/)

AWS and Microsoft are responsible for managing their infrastructure and services offered on top of that infrastructure, and Bizzdesign is responsible for configuration of the services ordered from AWS and Microsoft to support the System including logical access controls, encryption of data et cetera within those services. There is however one exception: The controls related to the following criteria are fully delegated to AWS and Microsoft:

CC6.4 - Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security.

AWS and Microsoft are SOC2 certified, including coverage of criteria CC6.4, and Bizzdesign has implemented a control to monitor for continued certification.

Attachment B – Bizzdesign's principal service commitments and system requirements

The principal service commitments and system requirements

This paragraph describes the service commitments which result in the described system requirements.

Trust Services Category	Service commitments	System requirements
Security	Customers require that the data they upload to the system is guarded by adequate security measures to guarantee confidentiality.	The system should prevent unauthorized access. The system should be monitored for availability and security. Customer data should be encrypted while at rest and when transmitted across the internet.
Availability	Customers demand that the system is available for use during their business hours with minimal downtime. Customers require adequate backups of their data to guard it against unexpected loss.	The system should be designed for at least 99,5% availability as defined in our SLA. Backups of customers data should be created at least once every 24 hours. The system should be monitored for availability and security.