SECURECYBERGATES LLP.

SOC 2 REPORT

For

SecureCyberGates Products – Cloud-Hosted Software Applications

TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY, CONFIDENTIALITY & AVAILABILITY

July 30, 2025 – October 31, 2025

Attestation and Compliance Services

<<VENDOR COMPANY LOGO FROM WHERE SOC2 ATTESTAION SERVICES ARE TAKEN>>

This report is intended solely for use by the management of SecureCyberGates LLP user entities of SecureCyberGates LLP’s services, and other parties who have sufficient knowledge and understanding of SecureCyberGates LLP’s services covered by this report (each referred to herein as a “specified user”).

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against <SOC2VENDOR> and the service auditor as a result of such access. Further, <SOC2VENDOR> and the service auditor do not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT

To Board of Directors
SecureCyberGates LLP.

Scope

We have examined the accompanying “Description of [SecureCyberGates] Products, cloud-hosted software applications” provided by [SecureCyberGates] LLP throughout the period July 30, 2025 to October 31, 2025 (the Description) and the suitability of the design and operating effectiveness of controls to meet [SecureCyberGates] LLP’s service commitments and system requirements based on the criteria for Security, Confidentiality, Availability, Processing Integrity & Privacy principles set forth in TSP Section 100 Principles and Criteria, Trust Services Principles and Criteria for Security, Confidentiality and Availability (applicable trust services criteria) throughout the period July 30, 2025 to October 31, 2025.

[SecureCyberGates] LLP uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-as-a-Service (SaaS), GitHub Inc., an open-core company that provides GitHub, a DevOps software package that combines the ability to develop, secure, and operate software in a single application, Microsoft Azure, a cloud computing service operated by Microsoft for application management and Microsoft Corporation (Office 365), a subservice organization, to provide office communication, file sharing, collaboration services and Microsoft Office applications like Word, Excel, and PowerPoint. The description presents [SecureCyberGates] LLP’s controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of [SecureCyberGates]’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.

The description presents [SecureCyberGates] LLP’s controls, the applicable trust services criteria and the types of complementary user entity controls assumed in the design of [SecureCyberGates] LLP’s controls. The description does not disclose the actual controls at the user entity organizations. Our examination did not include the services provided by the user entity organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization’s Responsibilities

[SecureCyberGates] LLP has provided the accompanying assertion titled “[SecureCyberGates] LLP’s Management Assertion throughout the period July 30, 2025 to October 31, 2025” about the fairness of the presentation of the Description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet [SecureCyberGates] LLP’s service commitments and system requirements based on the applicable trust services criteria. [SecureCyberGates] LLP 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 prevent the applicable trust services criteria from being met; (5) specifying the controls that meet [SecureCyberGates] LLP.'s service commitments and system requirements based on the applicable trust services criteria and stating them in the description; (6) designing, implementing, maintaining and documenting controls to meet [SecureCyberGates] LLP's service commitments and system requirements based on the applicable trust services criteria stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in [SecureCyberGates] LLP's assertion and on the suitability of the design and operating effectiveness of the controls to provide reasonable assurance that the service organizations commitments and system requirements were met based on applicable trust services criteria.

We conducted our examination 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 fairly presented based on the description criteria and (2) the controls were suitably designed to provide reasonable assurance that the service organization's commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria (3) the controls operated effectively to provide reasonable assurance that the service organization's commitments and system requirements were achieved based on the applicable trust services criteria throughout the period July 30, 2025 to October 31, 2025.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operated effectively to provide reasonable assurance that the service organization's commitments and system requirements meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the service organization's commitments and system requirements based on the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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 it's own particular needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria.

Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Description of tests of controls

In Section III, the specific controls tested and the nature and timing, and results of those tests are listed in the accompanying description of Criteria, Controls, Tests and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the description criteria described in [SecureCyberGates] LLP's assertion and the applicable trust services criteria:

a. The description fairly presents [SecureCyberGates] LLP's [SecureCyberGates] Products, cloud-hosted software applications, provided by [SecureCyberGates] LLP that was designed and implemented throughout the period July 30, 2025 to October 31, 2025.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the service organizations commitments and system requirements would be achieved if the controls operated effectively based on the applicable trust services criteria and if sub-service organizations and user entities applied the controls contemplated in the design of [SecureCyberGates] LLP's controls throughout the period July 30, 2025 to October 31, 2025.

c. The controls tested, which were those necessary to provide reasonable assurance that the service organizations commitments and system requirements based on the applicable trust services principles criteria were met, operated effectively throughout the period July 30, 2025 to October 31, 2025.

Restricted Use

This report, including the description of tests of controls and results thereof in the description of tests and results is intended solely for the information and use of user entities of [SecureCyberGates] LLP's, [SecureCyberGates] Products, cloud-hosted software applications throughout the period July 30, 2025 to October 31, 2025, and prospective user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organizations' system interacts with the user entities, subservice organizations, or other parties.
- Internal controls and its limitations.
- Complementary subservice organizations and complementary user entity controls and how those controls interact with the controls at the service organizations to achieve the service organization's service commitments and system requirements.
- 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.

<CPA Attestation Here>

CPA NAME
Certified Public Accountant
License Number: #####
July 30, 2025

SECTION 2

MANAGEMENT’S ASSERTION

MANAGEMENT ‘S ASSERTION

[SecureCyberGates] LLP’s Management Assertion throughout the period July 30, 2025 to October 31, 2025

We have prepared the attached description titled “Description of [SecureCyberGates] LLP’s [SecureCyberGates] Products, cloud-hosted software applications” throughout the period July 30, 2025 to October 31, 2025 (the description), based on the criteria in items (a) (i)–(ii) below, which are the criteria for a description of a service organization’s system given in DC Section 200 prepared by AICPA’s Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force’s SOC 2® Guide Working Group to be used in conjunction with the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the [SecureCyberGates] LLP, [SecureCyberGates] Products, cloud-hosted software applications provided by [SecureCyberGates] LLP that may be useful when assessing the risks from interactions with the system throughout the period July 30, 2025 to October 31, 2025 particularly information about the suitability of the design and operating effectiveness of controls to meet [SecureCyberGates] LLP’s service commitments and system requirements based on the criteria related to Security, Confidentiality & 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).*

[SecureCyberGates] LLP uses Amazon Web Services Inc. (AWS), a subservice organization, to provide cloud Software-As-A-Service (SaaS), GitHub Inc., an open-core company that provides Github, a DevOps software package that combines the ability to develop, secure, and operate software in a single application, Microsoft Azure, a cloud computing service operated by Microsoft for application management and Microsoft Corporation (Office 365), a subservice organization, to provide office communication, file sharing, collaboration services and Microsoft Office applications like Word, Excel, and PowerPoint. The description presents [SecureCyberGates] LLP’s controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of [SecureCyberGates] LLP’s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity organization controls that are suitably designed and operating effectively are necessary, along with controls at [SecureCyberGates] LLP to achieve [SecureCyberGates] LLP’s service commitments and system requirements based on the applicable trust services criteria. The description presents [SecureCyberGates] LLP’s controls, the applicable trust services criteria and the types of complementary user entity organization controls assumed in the design of [SecureCyberGates] LLP’s controls. The description does not disclose the actual controls at the user entity organizations.

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

1. The description of [SecureCyberGates] LLP, [SecureCyberGates] Products, cloud-hosted software applications, provided by [SecureCyberGates] LLP throughout the period July 30, 2025 to October 31, 2025 the criteria for description are identified below under the heading “Description Criteria”.

2. The controls stated in the description were suitably designed and operated effectively to meet [SecureCyberGates] LLP’s service commitments and system requirements based on the applicable trust services criteria throughout the period July 30, 2025 to October 31, 2025, to meet the applicable trust services criteria.

Description Criteria:

i. The description contains the following information:

   1. The types of services provided.
   2. The principal service commitments and system requirements.
   3. The components of the system used to provide the services, which are the following:
      - Infrastructure - The physical and hardware components of a system (facilities, equipment, and networks).
      - Software - The programs and operating software of a system (systems, applications, and utilities).
      - People - The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - Procedures - The automated and manual procedures involved in the operation of a system.
      - Data - The information used and supported by a system (transaction streams, files, databases, and tables).
   4. The boundaries or aspects of the system are covered by the description.
   5. The applicable trust services criteria and the related controls are designed to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved.

6. Other aspects of the service organization’s control environment, risk assessment process, communication and information systems and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

ii. The description does not omit or distort information relevant to the service organizations’ system while acknowledging that 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 his or her own needs.

For [SecureCyberGates] LLP

AJ KHAN

AJ KHAN [CISO, [SecureCyberGates] LLP]
July 28, 2025
--
Authorized Signatory

SECTION 3

SYSTEM'S DESCRIPTION

[Note : This is just sample System description and DOES NOT represent JurisTech Original Systems. All data are Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

1) Overview of Operations

At JurisTech, we are more than just a software company; we are a driving force behind the digital transformation of the financial world. As a global leader in enterprise-class lending and recovery solutions, we empower banks, financial institutions, telecommunications, and automotive companies worldwide to thrive in a rapidly evolving landscape.

Our journey began during the turbulence of the 1997 Asian financial crisis, a period that shaped our commitment to innovation and resilience. Since then, we have grown into a pioneer, delivering cutting-edge software solutions that harness the power of artificial intelligence (AI), conversational chatbots, digital onboarding, and more. From loan origination and credit scoring to debt collection and litigation, we partner with banks and financial institutions to redefine the future of finance. Our solutions do not just adapt to change; they drive it. By enabling digital transformation, we ensure our clients provide an unparalleled customer experience while achieving their business goals with confidence.

[Content Copied from publically available resource https://juristech.net/juristech/about-us/]

1.1) Description of Services Provided

Buiseness

Our business goals focus on being globally as well as locally. At JurisTech, we offer our in-house specialists to align with our client's goal; either in understanding the Malaysian Shariah's law, or complex compliance process of international regulation. At the very heart of JurisTech, we believe in identifying the root cause of a business issue in order to come up with a befitting solution. With a multinational workforce, we are sensitive to the diverse customer's journey and aim to bring our best game in software implementation in the Fintech industry.

Product Design and Development: Our R&D and product teams put innovation at the heart of our solutions, ensuring every product conforms to the market standards.

Project Delivery Capability: We offer extensive support for pre, during, and post-project implementation to ensure the client's goals are met and fulfilled.

International Delivery Capabilities: Our sustainable and agile business operations, processes, and decision-making has been strategically optimised to cater to the international market with different time zones.

Financial Industry Knowledge and Expertise/ Tech Leader: Headed by See Wai Hun, JurisTech's visionary CEO (also named as EY Woman Entrepreneur Of The Year 2019 in Malaysia), our team of financial and tech experts diligently fulfil client's requirements to not only transform your existing system but also revolutionise your digital processes.

Governance & Compliance: One of the advantages of working with us is our in-house specialists' expertise on Islamic banking and Shariah compliance regulations, on top of being sensitive to local regulations where the project is implemented or based at.

Quality Assurance Service/Quality Management: Quality control and management during a system implementation are critical aspects in ensuring every project is executed successfully. We ensure every implementation is managed thoroughly for the highest quality assurance and deliverables.

[Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

Technical
JurisTech prides itself on its technical innovation across all our solutions over the years. JurisTech's solutions are designed and developed using the Juris Solutions Interaction Platform (JSIP) which is built on-top of the Juris Application Server (JAS). JAS consists of an integrated framework of highly scalable components which is used to build enterprise-strength solutions.

JurisTech's technical capabilities have many times proven to set highly competitive standards to all our clients to create seamless and secure service streams across their customer channels. With our technology, we aim to deliver the best-in-class solutions to serve our clients operational excellence.

Low Code Technology Our solutions are supported by powerful front-end frameworks that do not require advanced coding capabilities.

Powerful Workflow Engine Our solutions are backed with a robust infrastructure, Juris Workflow Engine, engineered with the flexibility to manage and design different workflows that accommodate different target markets (banks/non-banks).

Multi-channel Integration and API-powered Our solutions enable straight-through processing capabilities and are inclusive of the entire digital ecosystem in the market.

Multi-tenancy Control Our solutions come with multiple tenancy controls on all major tables such as user access matrixes, user management, user workflows and applications with the ability to segregate each tenancy with its own setups and data in a single instance.

Application Security Juris SecureGuard Security Framework was built to uphold security measures and encrypt customer sensitive information against threats such as Input Filtering of XSS, SQL Injection attacks, DDoS attacks, Cross-site scripting across all our solutions. Juris SecureGuard also conforms with all regulatory requirements in every region.

Disaster Recovery Our solutions run on systematic protocols to overturn several different adversities such as network outages, transaction rollbacks, and out of memory errors.

[Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

Delivery and Support
We appreciate the complexity of every project implementation and always strive to deliver our best in supporting our clients' transformation. We understand behind every successful project execution; it is crucial to ensure sufficient post-project support for a smooth transition.

Help Desk Our cooperative help desk personnel are always ready to walk you through any pertaining issues at any stage of the project lifecycle, making sure your support needs are met and fulfilled.

Advocates for Client Experience and Success (ACES) Back up by an extensive team of technical personnel with diverse knowledge of the industry from our HQ assisted by our off-site team in Uganda, we offer end-to-end post-implementation guidelines to help you navigate through your newly enhanced system based on project requirements, organisational needs, etc.

Training & Resources Training and resources are adequately given and delivered throughout the project implementation and post-execution to support your transition into the newly implemented system.

Service Level Agreement Client satisfaction is always at the top of our priorities; we fulfil our obligations and deliver on our promises 100%. We strive to achieve mutual understanding in terms of performance standards to establish a positive experience for all involved parties.

[Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

2) List of Products
[Copied from publically available resource https://juristech.net/juristech/solutions/]

Digital Onboarding

Product Name	Description
Juris Access	Juris Access is a digital customer onboarding platform, that enables financial institutions or companies to create an engaging end-to-end onboarding journey. Built to accelerate your customers' financial-related applications, Juris Access digitally onboards them by facilitating customer acquisition, application, eligibility pre-screening, and evaluation for financial and credit products. https://juristech.net/juristech/juris-access/
Juris DecisionCraft	Juris DecisionCraft is an auto-decisioning engine that orchestrates and synergises different data and analytics from different systems or

	sources to produce the best decision possible. https://juristech.net/juristech/juris-decisioncraft/
Juris V-Box	Juris V-Box is an instant, secure document request and collaboration platform, that enables financial institutions or agents/partners to request, collect, track and secure customers' documents. https://juristech.net/juristech/juris-v-box/
Juris Anny	Juris Anny is an intelligent chatbot with natural language processing (NLP) specifically engineered to cater to financial service-related questions and transactional requests. https://juristech.net/juristech/juris-anny/
Financial Services Marketing	Specialised marketing solutions for financial services providers https://juristech.net/juristech/financial-services-marketing/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Digital Lending

Product Name	Description
Juris Origination	Juris Origination is a loan origination system that automates the entire loan application and approval process. The system drastically simplifies the process from application, scoring, evaluation, underwriting, approval, acceptance, documentation, up to disbursement. https://juristech.net/juristech/juris-origination/
Juris Credit	Juris Credit is a credit administration platform that unifies and manages the entire credit process workflow of valuers, solicitors and financial institutions in a single platform. https://juristech.net/juristech/juris-credit/
Juris Analyst	Juris Analyst is a financial evaluation system for businesses that simulates, evaluates, and forecasts your clients' financial health and their repayment ability. It provides data feed to scoring and risk rating systems and intelligently analyses company financial positions over a desired period, including the past, present and future. https://juristech.net/juristech/juris-analyst/
Juris OneCore	Juris OneCore is an end-to-end loan management solution that is built with small and medium-size lenders in mind, empowering these businesses to effectively manage loan or financing products offerings. It is built to encompass the full lifecycle of loan management, including application creation, reconciliations, loan rescheduling, loan settlements and write-offs. https://juristech.net/juristech/juris-onecore/
Juris Leads	Juris Leads is a lead management system that captures, tracks, and nurtures prospects and existing customers, to be converted into new business opportunities. It captures leads from multiple channels and sources, automatically distributes to the right relationship manager and create a centralised platform to manage prospects and customers'

	conversion journey. https://juristech.net/juristech/juris-leads/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Collection and Recovery

Product Name	Description
Juris Collect	Juris Collect is an end-to-end enterprise debt collection system that handles early delinquent accounts to late-stage accounts, whilst intelligently employing personalised collection strategies for different customer profiles. https://juristech.net/juristech/juris-collect/
Juris Legal	Juris Legal is a legal workflow management platform for late-stage recovery, connecting financial institutions and law firms. It helps financial institutions to streamline and optimise the standard civil suit and foreclosure litigation processes by automating case distribution, billing and approval processes, and most importantly, providing a platform for law firms to collaborate real-time on litigation matters. https://juristech.net/juristech/juris-legal/
Juris Predator	Juris Predator is an all-in-one computer-telephony integration (CTI) software equipped with powerful diallers, inbound call routing and comprehensive information tracking. It is able to turn your computer into a telephone call management system centralising control over all call-related tasks with powerful and intelligent outbound dialling modes options – preview, progressive and predictive dialling. https://juristech.net/juristech/juris-predator/
Nexcoll	The one-stop software solution for debt collection agencies — with web-based access that lets you login from anywhere, anytime! https://nexcoll.my/nexcoll/
Collectxpress	Cloud-based collection software that manages and keeps track of all your invoices without ever missing a customer's payment. https://collectxpress.net/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Artificial Intelligence

Product Name	Description
Juris AICraft	Juris AICraft is an Agentic AI platform that integrates diverse AI capabilities to deliver tailored solutions for your evolving business needs. Each AI technology operates as independent modules, collaborating like specialised agents to solve complex business challenges. https://juristech.net/juristech/juris-aicraft/
Juris MindCraft	Juris Mindcraft is an automated Machine Learning (autoML) and

	artificial intelligence (AI) platform that uses advanced machine learning (ML) techniques to build powerful AI models. An effortless AI that enables enterprises especially banks and financial institutions to make intelligent business decisions and gain insights to solve real-world problems. https://juristech.net/juristech/juris-mindcraft/
Juris Spectrum	Juris Spectrum is an end-to-end digital banking platform, offering a unique, holistic digital banking experience for customers and businesses. Powered by connectivity and agility, Juris Spectrum is composed of a robust digital core and state-of-the-art customer engagement, lending, deposits, and collection capabilities. https://juristech.net/juristech/juris-spectrum/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

3) Principal Service Commitments and System Requirements

JurisTech designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that JurisTech makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that JurisTech has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- ✓ The fundamental design of JurisTech's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- ✓ JurisTech implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- ✓ Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.
- ✓ Internal and External Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- ✓ Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- ✓ The use of encryption technologies to protect system data both at rest and in transit.
- ✓ Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- ✓ Confidential information must be used only for the purposes explicitly stated in agreements between JurisTech and user entities.

Availability commitments include, but are not limited to, the following:

- ✓ System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- ✓ Responding to customer requests in a reasonably timely manner.
- ✓ Business continuity and disaster recovery plans and,
- ✓ Operational procedures supporting the achievement of availability commitments to user entities.

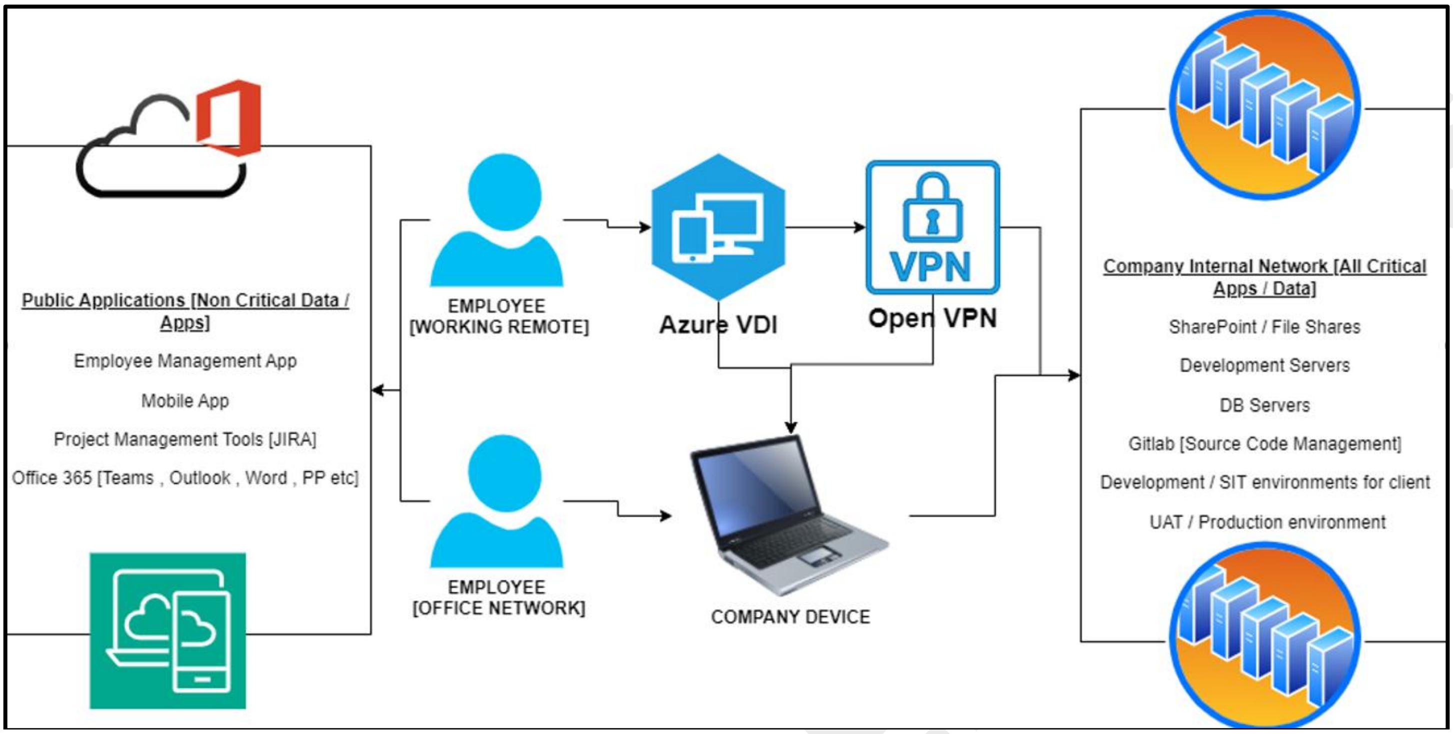
Such requirements are communicated in JurisTech 's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

4) Components of the System used to provide services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below:

Infrastructure
Software
People
Data
Policies and Procedures

4.1) Infrastructure


Public Applications [Non Critical Data / Apps]
Employee Management App
Mobile App
Project Management Tools [JIRA]
Office 365 [Teams , Outlook , Word , PP etc]
EMPLOYEE [WORKING REMOTE]
EMPLOYEE [OFFICE NETWORK]
Azure VDI
VPN
Open VPN
COMPANY DEVICE
Company Internal Network [All Critical Apps / Data]
SharePoint / File Shares
Development Servers
DB Servers
Gitlab [Source Code Management]
Development / SIT environments for client
UAT / Production environment

NOTE: This diagram is just a sample one and does NOT represent JurisTech

Company Data is hosted on Premise [e.g. Development Servers, Internal applications like Employee management [Employee Attendance, Their Details, Leaves etc.]

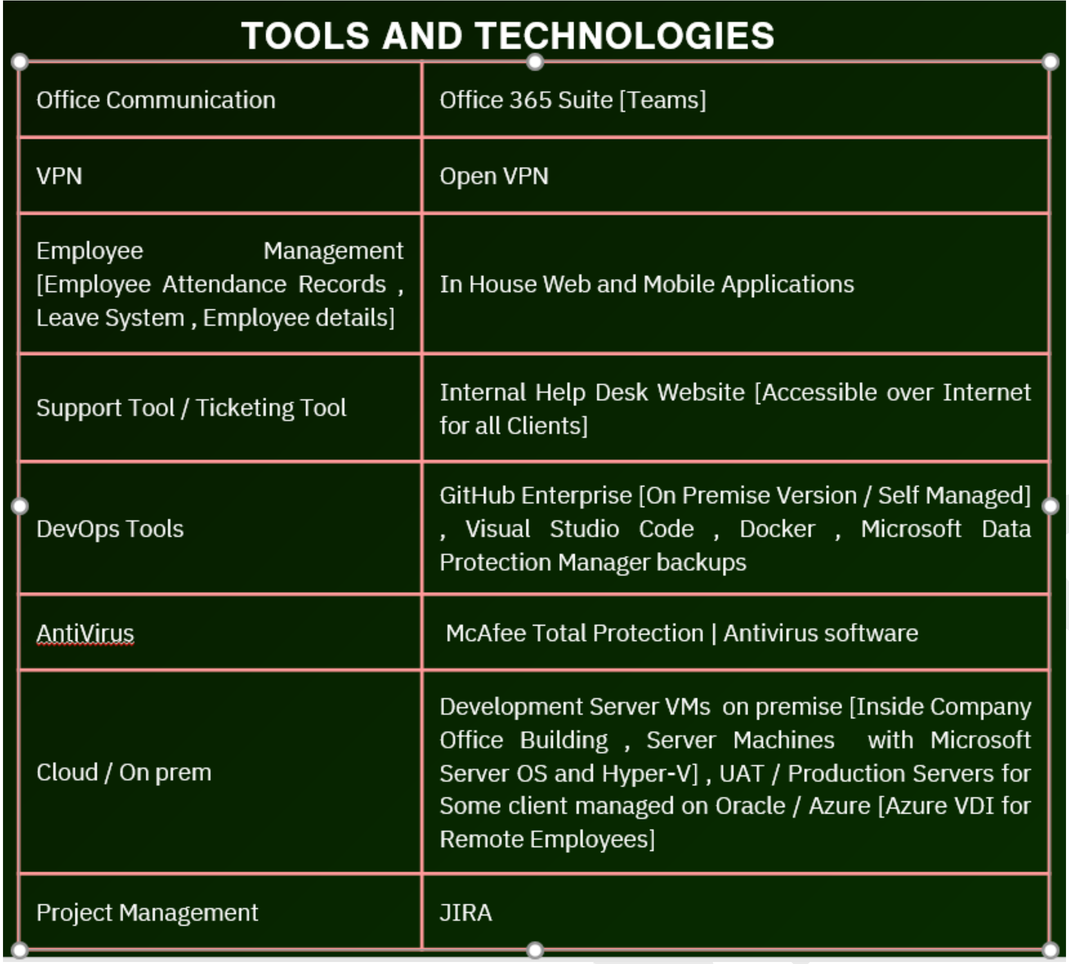
Some Company Data is hosted on Cloud e.g. Company uses JIRA Cloud , Some data on Azure Cloud, Some on AWS cloud , Company uses Office 365 products for daily Communication]

Customer Data is managed by Customers. e.g. JurisTech develop Loan management Software and deliver the product to Customer [Now all Production Data is responsibility of Customer] . Some of these cients have asked JursTech to handle their own Customer data for this JurisTech uses Azure , AWS , Google and Oracle Cloud

4.2) Software

Kindly refer List of products at https://juristech.net/juristech/solutions/

Technical Security Controls



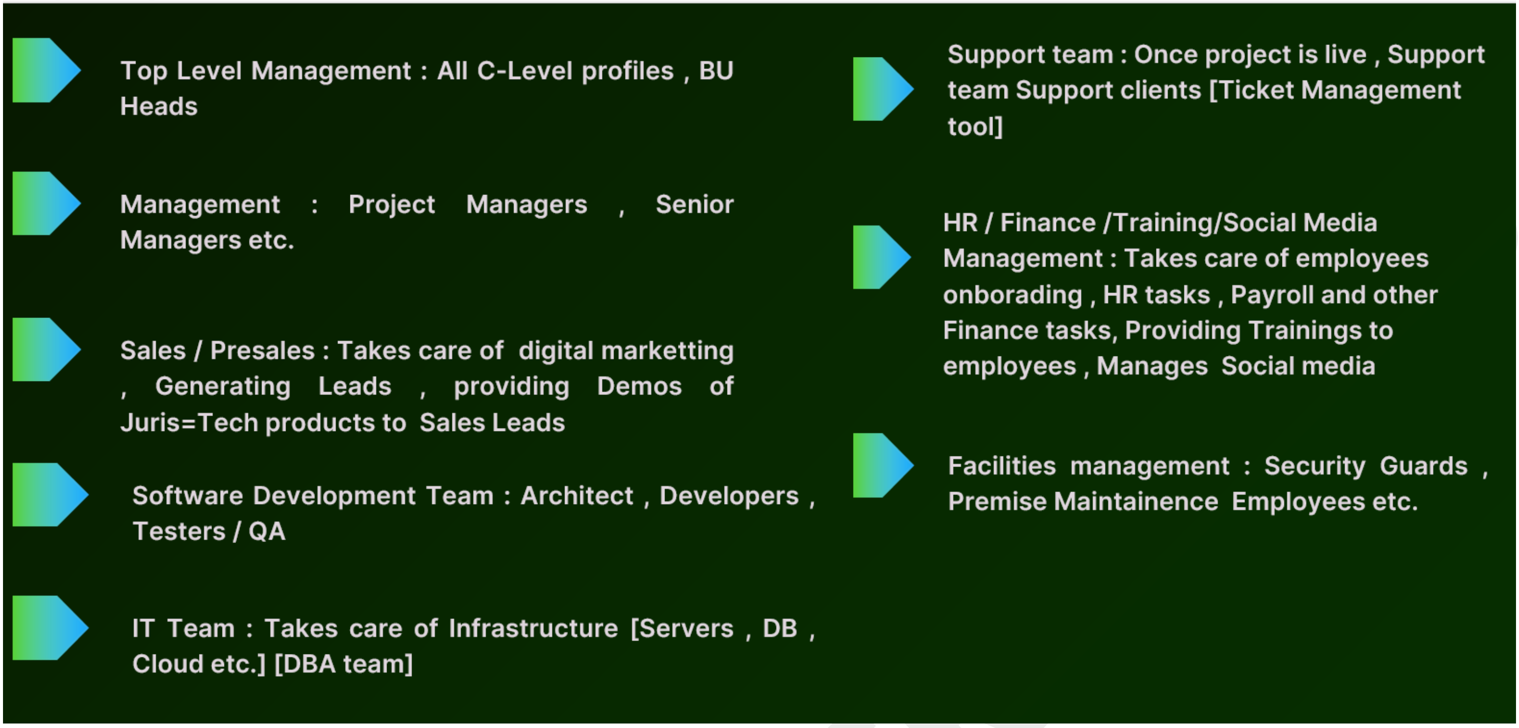
TOOLS AND TECHNOLOGIES

Office Communication	Office 365 Suite [Teams]
VPN	Open VPN
Employee Management [Employee Attendance Records , Leave System , Employee details]	In House Web and Mobile Applications
Support Tool / Ticketing Tool	Internal Help Desk Website [Accessible over Internet for all Clients]
DevOps Tools	GitHub Enterprise [On Premise Version / Self Managed] , Visual Studio Code , Docker , Microsoft Data Protection Manager backups
AntiVirus	McAfee Total Protection | Antivirus software
Cloud / On prem	Development Server VMs on premise [Inside Company Office Building , Server Machines with Microsoft Server OS and Hyper-V] , UAT / Production Servers for Some client managed on Oracle / Azure [Azure VDI for Remote Employees]
Project Management	JIRA

Tool used	Description
Microsoft Threat Modeling Tool	Threat modelling at design Phase.
GitHub CodeQL	GitHub SAST (Static Application Security Testing)
Sonatype Nexus IQ	Open-source vulnerabilities
BurpSuite	DAST tool
OWASP ZAP	DAST tool
Azure Sentinel	SIEM and SOAR tool
Azure /AWS/ Oracle WAF	Web application Firewall
Cisco Secure Firewall 4200 Series	Physical firewall for Office-premise network
OWASP TOP 10	Approach for Security Testing

NOTE: This Table/diagram is just a sample one and does NOT represent JurisTech real systems.

4.3) People



Top Level Management : All C-Level profiles , BU Heads

Management : Project Managers , Senior Managers etc.

Sales / Presales : Takes care of digital marketting , Generating Leads , providing Demos of Juris=Tech products to Sales Leads

Software Development Team : Architect , Developers , Testers / QA

IT Team : Takes care of Infrastructure [Servers , DB , Cloud etc.] [DBA team]

Support team : Once project is live , Support team Support clients [Ticket Management tool]

HR / Finance /Training/Social Media Management : Takes care of employees onborading , HR tasks , Payroll and other Finance tasks, Providing Trainings to employees , Manages Social media

Facilities management : Security Guards , Premise Maintainence Employees etc.

4.4) Data

Data, as defined by JurisTech, constitutes the following:
Company Data [All Data related to Company Phone number, email Ids etc.]
Customer Data [Any data specific to customer, customer details, Projects etc.]
Application Data [Source code, Project Documents, Reports etc.]
Environment details [Development, SIT/UAT, Production environment details etc.]
System files
Audit and Error logs

Any Confidential Data / Reports delivered externally are only sent using a secure method—encrypted email, secure FTP, or secure websites to customer users.

All data that is managed, processed and stored as a part of the JurisTech software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements.	Customer system and operating data Customer PII Anything subject to a confidentiality agreement with a customer

	Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	
Company Confidential	Information that originated or is owned internally, or was entrusted to JurisTech by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	JurisTech's PII Unpublished financial information Documents and processes explicitly marked as confidential Unpublished goals, forecasts, and initiatives marked as confidential Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	Press releases Public website

Customer data is retained per agreements with customers and disposed of upon request by customers. A confirmation is sent back to the customer to notify them that the disposal is complete

4.5) Policies and Procedures

Formal policies and procedures have been established to support the JurisTech software application. These policies cover:

Code of Business Conduct
Change Management
Data Retention
Data Backup
Information security
Vendor management
Physical security
Risk management
Password
Media disposal
Incident management
Endpoint security
Encryption
Disaster recovery
Data classification
Confidentiality

Business continuity
Access control
Acceptable usage
Vulnerability management
Human Resource Management

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

JurisTech also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the JurisTech software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

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

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part JurisTech 's description of the system. This section provides information about the five interrelated components of internal control at JurisTech, including:

- ✓ Control environment
- ✓ Risk assessment
- ✓ Control activities
- ✓ Information and communication
- ✓ Monitoring controls

5.1) Control environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of JurisTech's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of JurisTech's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

JurisTech and its management team has established the following controls to incorporate ethical values throughout the organization:

- ✓ A formally documented “Code of business conduct” communicates the organization’s values and behavioral standards to staff members
- ✓ Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- ✓ All new employees go through background checks as a part of the hiring process.

Commitment to Competence

JurisTech’s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees’ roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.

- ✓ Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- ✓ Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- ✓ Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Senior Management Oversight

JurisTech’s control awareness is significantly influenced by its senior management. Attributes that define “tone at the top” include senior management’s experience of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company’s operations and information security posture.

Management Philosophy and Operating Style

JurisTech’s management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management’s approach to monitoring business risks, and management’s attitudes toward personnel and the processing of information. JurisTech’s control environment reflects the philosophy of management. JurisTech 's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities JurisTech has implemented in this area are described below:

Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high severity security incidents annually.
Senior management meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap.

Organizational Structure and Assignment of Authority and Responsibility

JurisTech's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and updated as required.

Human Resources

JurisTech's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top quality personnel who ensure the service organization operates at maximum efficiency.

Specific control activities that the service organization has implemented in this area are described below:

- ✓ Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- ✓ Job positions are supported by job descriptions.
- ✓ New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- ✓ Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- ✓ Performance evaluations for each employee are performed on an annual basis.
- ✓ If an employee violates the Code of Conduct in the employee handbook or the company's
- ✓ Policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

5.2) Risk assessment

JurisTech regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the 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).

JurisTech's risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. JurisTech identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks. This process identifies risks to the services provided by the JurisTech Software application, Data, Infrastructure and management has implemented various measures designed to manage these risks

JurisTech believes that effective risk management is based on the following principles:

- ✓ Senior management's commitment to the security of JurisTech assets [Software, Data, Infra, Documents etc.]
- ✓ The involvement, cooperation, and insight of all JurisTech staff.
- ✓ Initiating risk assessments with discovery and identification of risks.
- ✓ Thorough analysis of identified risks.
- ✓ Commitment to the strategy and treatment of identified risks.
- ✓ Communicating all identified risks to the senior management.
- ✓ Encouraging all JurisTech staff to report risks and threat vectors.

Scope

The risk assessment and management program applies to all systems and data that are a part of the JurisTech assets [Software, Data, Infra, Documents etc.]. The JurisTech risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.
Risk assessments may be high level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.
Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of JurisTech's Information Security Officer and the department or individuals responsible for the area being assessed. All JurisTech staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

JurisTech uses a number of vendors to meet its business objectives. JurisTech understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.
JurisTech employs several activities to effectively manage their vendors. Information Security

Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, JurisTech assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support JurisTech's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, JurisTech management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, JurisTech identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. JurisTech's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity and mitigating action.

5.3) Control activities

JurisTech's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

The JurisTech software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

JurisTech has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

Administrator access to the production console is restricted to authorized system and security administrators. Powerful service/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.
Staff members must use complex passwords, wherever possible, for all of their accounts that have access to JurisTech customer data. Staff are encouraged to use passwords which have at least 12 characters, randomly generated, alphanumeric and special-character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems requires multi-factor authentication (MFA). Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Physical Access and Environmental Controls
JurisTech has a well-rounded physicals security in place to protect the site, the equipment and underlying software from any physical damage such as vandalism, theft and other accidents. The business suite that houses our office as well as our own premises has 24-hour CCTV surveillance and controlled access. Only authorized personnel can enter the office premises, and this is validated via a bio-metric access system. All individual laptops and workstations are password protected and the responsibility of JurisTech employees. The servers and other systems maintained by JurisTech are in a secure environment and not all employees are provided access. Only authorized and relevant users with need-to-have access are allowed. Smoke detectors and relevant fire suppression systems are in place and periodically tested and go through maintenance cycles. Overall, physical security measures are taken care of by both the building management and JurisTech.

Incident Management
JurisTech has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact JurisTech via support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.
Incident response procedures and centralized tracking tools [Juris Gold] consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.
Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- ✓ **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of JurisTech being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.

- ✓ **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.
- ✓ **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- ✓ **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. Incidents and alerts from the security utilities are reviewed by FIS and Security team. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

JurisTech only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to JurisTech's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to JurisTech web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using strong algorithms like Advanced Encryption Standard (AES) 256 bit.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the JurisTech are reviewed, deployed, and managed. The policy covers all changes made to the JurisTech software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- ✓ Corrupted or destroyed information
- ✓ Degraded or disrupted software application performance

- ✓ Productivity loss
- ✓ Introduction of software bugs, configuration errors, vulnerabilities, etc.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities. ServiceNow software are used for change request management. Customer content and personal information are not used in non-production environments.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management

Vulnerability scanning tools are used to scan systems on the application, network to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

Anti-malware software [McaFee] to continuously monitor and defend each of the organization's workstations and servers.

Availability

JurisTech has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). Frequent Backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

5.4) Information and Communication

JurisTech maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, JurisTech also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Information about the system and services are maintained and made available to users on the company website.

5.5) Monitoring controls

JurisTech's management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored.

This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Disclosure of Incidents

There were no system incidents as of JANUARY 01 2025 to JUNE 15th 2025, requiring disclosure that either:

Were the result of controls failing; or,

Resulted in a significant impairment to the achievement of system requirements or service commitments to customers.

Complementary User Entity Controls

JurisTech's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for JurisTech customers.

For customers to rely on the information processed through the JurisTech's software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- ✓ User entity is responsible for managing their organization's JurisTech's Products account as well as establishing any customized security solutions or automated processes through the use of setup features
- ✓ User entity is responsible for protecting established user IDs and passwords within their organizations.
- ✓ User entity is responsible for reviewing customer access to the JurisTech's Products application periodically to validate appropriateness of access levels.
- ✓ User entity is responsible for approving and creating new user access to the

JurisTech's Products Software application.

- ✓ User entity is responsible for removing terminated employee access to the JurisTech's Products software application.
- ✓ User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the JurisTech's Products software application.
- ✓ User entity is responsible for sending data to JurisTech's software application via a secure connection and/or the data should be encrypted.
- ✓ User entity is responsible for notifying JurisTech's Products software application if they detect or suspect a security incident related to the JurisTech
- ✓ User entity is responsible for reviewing email and other forms of communications from JurisTech related to changes that may affect JurisTech customers and users, and their security or availability obligations.
- ✓ User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- ✓ User entity is responsible for endpoint protection of workstations used to access the system.
- ✓ User entity is responsible for developing their own business continuity and disaster recovery plan.

[Note : This is just sample System description and DOES NOT represent JurisTech Original Systems.]

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report is on the controls relating to the [SecureCyberGates] LLP. [SecureCyberGates] Products, cloud-hosted software applications provided by [SecureCyberGates] LLP. The scope of the testing was restricted to [SecureCyberGates] LLP. [SecureCyberGates] Products, cloud-hosted software applications, and its boundaries as defined in Section 3. [SecureCyberGates] LLP. conducted the examination testing throughout the period July 30, 2025 to October 31, 2025.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, [SECURECYBERGATES] LLP. considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk is mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, [SOC2VENDORCOMPANY] utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. [SOC2VENDORCOMPANY], in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: CONTROL ENVIRONMENT			
CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	**Entity has a documented policy to define behavioral standards and acceptable business conduct.**	**Inspected the Company Procedure & Policies to determine the behavioral standards and acceptable business conduct [AUP].** **Observed that it has been reviewed and acknowledged by staff members.**	**No exceptions noted.**
CC1.1.2	**Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.**	**Inspected the Company Procedure & Policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.** **Observed that the policies have been reviewed and acknowledged by new staff members.**	**No exceptions noted.**
CC1.1.3	**Entity outlines and documents cybersecurity responsibilities for all personnel.**	**Inspected Information Security Policy to determine that the entity outlines and documents cybersecurity responsibilities for all personnel.**	**No exceptions noted.**
CC1.1.4	**Entity establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet.**	**Inspected Code of Conduct Policy.**	**No exceptions noted.**
CC1.1.5	**Entity has established procedures for staff to acknowledge applicable company policies periodically.**	**Inspected the Company Procedure & Policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically.** **Inspected records that the policies have been reviewed and acknowledged by staff**	**No exceptions noted.**

		members.	
CC1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	**Entity's Senior Management reviews and approves all company policies annually.**	**Inspected that the company policies have been reviewed and approved by Senior Management.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.2	**Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.**	**Inspected that the Senior Management has reviewed and approved the entity's Organizational Structure.** **Evidenced Organization chart.**	**No exceptions noted.**
CC1.2.3	**Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.**	**Inspected the Risk Management Process showing that the Senior Management has reviewed and approved the documents.** **Evidenced Risk register.**	**No exceptions noted.**
CC1.2.4	**Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.**	**Evidenced Risk register.**	**No exceptions noted.**
CC1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	**Entity has established procedures to communicate with staff about their roles and responsibilities.**	**Inspected Roles & job descriptions document to determine that the entity has established procedures to communicate with staff about their roles and responsibilities.**	**No exceptions noted.**
CC1.3.2	**Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.**	**Inspected the CISO Appointment Letter showing that the role of Information Security Officer has been appropriately assigned.**	**No exceptions noted.**

CC1.3.3	**Entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.**	**Inspected the company Organizational chart which shows reporting structure by role to determine that the entity maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.** **Evidenced Organization chart.**	**No exceptions noted.**
CC1.3.4	**Entity ensures clarity in job responsibilities for client serving, IT and engineering positions (via OKRs, Job Descriptions etc.) to increase the operational effectiveness of the organization.**	**Inspected Roles and job descriptions document to determine that the entity ensures clarity in job responsibilities.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	**Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.**	**Inspected the Roles & job descriptions document to determine that the entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.** **Evidenced security awareness training document.**	**No exceptions noted.**
CC1.4.2	**Entity has established procedures to perform security risk screening of individuals prior to authorizing access.**	**Inspected the HR Policy to determine that the entity has established procedures to perform security risk screening of individuals prior to authorizing access.**	**No exceptions noted.**
CC1.4.3	**Entity documents the formal recruiting process as per the policy and procedure defined to manage recruitment.**	**Inspected HR Policy to determine that the entity documents the formal recruiting process as per the policy and procedure defined to manage recruitment.**	**No exceptions noted.**
CC1.4.4	**Entity ensures that new hires go through a background check as part of their onboarding process.**	**Observed Background verification of employees to determine that the entity ensures that new hires go through a background check as part of their onboarding process.** **Evidenced Roles and job descriptions document.**	**No exceptions noted.**
CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.1	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Observed that the Information security awareness training has been completed by staff members to determine that the entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
CC1.5.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the Company Procedure & Policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC1.5.3	Entity requires that all staff members complete Information Security Awareness training annually.	Observed that the Information security awareness training has been completed by staff members to determine that the entity requires that all staff members complete Information Security Awareness training.	No exceptions noted.
CC1.5.4	Entity documents, monitors and retains individual training activities and records.	Inspected the security awareness training document.	No exceptions noted.
CC1.5.5	Entity provides information security and privacy training to staff that is relevant for their job function.	Inspected HR Policy to determine that the entity provides information security and privacy training to staff that is relevant for their job function.	No exceptions noted.
CC1.5.6	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their Job responsibilities.	Evidenced Roles and job descriptions document to determine that the entity requires Information security roles are periodically evaluated regarding their Job responsibilities.	No exceptions noted.
CC2.0: COMMUNICATION AND INFORMATION			
CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Inspected the monitoring alert configurations and the functioning of internal controls to determine that the entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal	No exceptions noted.

		controls. Evidenced Communication channels within Information Security Policy.	
CC2.1.2	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC2.1.3	Entity displays the most current information about its services on its website, which is accessible to its customers.	Inspected the company's website to determine that the entity displays the most current information about its services on its website, which is accessible to its customers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Observed that the Information security awareness training has been completed by staff members to determine that the entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No exceptions noted.
CC2.2.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the Company Procedure & Policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC2.2.3	Entity makes all policies and procedures available to all staff members for their perusal.	Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff members for their perusal.	No exceptions noted.
CC2.2.4	Entity requires that all staff members complete Information Security Awareness training annually.	Observed that the Information security awareness training has been completed by staff members to determine that the entity requires that all staff members complete Information Security Awareness training.	No exceptions noted.
CC2.2.5	Entity documents, monitors and retains individual training activities and records.	Inspected the security awareness training document.	No exceptions noted.

CC2.2.6	**Entity has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.**	**Inspected Information Security Policies document and Management of information security incidents and improvements document.**	**No exceptions noted.**
CC2.2.7	**Entity has a documented policy to define behavioral standards and acceptable business conduct.**	**Inspected the Company Procedure & Policies to determine the behavioral standards and acceptable business conduct.** **Observed that it has been reviewed and acknowledged by staff members.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.8	**Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.**	**Inspected the Company Procedure & Policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.** **Observed that the policies have been reviewed and acknowledged by new staff members.**	**No exceptions noted.**
CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	**Entity displays the most current information about its services on its website, which is accessible to its customers.**	**Inspected the company's website to determine that the entity displays the most current information about its services on its website, which is accessible to its customers.**	**No exceptions noted.**
CC2.3.2	**Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are**	**Observed Incident reports and Investigation records for security incidents and breaches document to determine that the entity has provided information to customers on how to report failures, incidents,**	**No exceptions noted.**

	problems.	**concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.**	
CC3.0: RISK ASSESSMENT			
CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	**Entity has formally documented policies and procedures to govern risk management.**	**Inspected the Risk Management Process document.**	**No exceptions noted.**
CC3.1.2	**Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.**	**Inspected the Risk Management Process to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.** **Verified the Risk register.**	**No exceptions noted.**
CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	**Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.**	**Inspected the Risk Management Process to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.** **Verified the Risk register.**	**No exceptions noted.**
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2.2	**Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and**	**Inspected the Risk Management Process to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring**	**No exceptions noted.**

	confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	and the potential impact on the security, availability, and confidentiality of the Company platform. Evidenced Risk register.	
CC3.2.3	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the Company Procedure & Policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC3.2.4	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the Risk Management Process and Records of Third-Party vendor and service provider assessments to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements. Evidenced Risk register.	No exceptions noted.
CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Entity considers the potential for fraud when assessing risks.	Inspected the Risk Management Process to determine that the entity considers the potential for fraud when assessing risks. Evidenced Risk register.	No exceptions noted.
CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and	Inspected the Risk Management Process to determine that the entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify	No exceptions noted.

	requirements.	threats that could impair systems' security commitments and requirements. Verified the Risk register.	
CC3.4.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the Risk Management Process to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Evidenced Risk register.	No exceptions noted.
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.4.3	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the Risk Management Process and Records of Third-Party vendor and service provider assessments to determine that the entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements. Evidenced Risk register.	No exceptions noted.
CC4.0: MONITORING ACTIVITIES			
CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the CISO Appointment Letter showing that the role of Information Security Officer has been appropriately assigned to determine that the Senior Management assigns the role of Information Security Officer who is delegated to centrally-	No exceptions noted.

		manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	
CC4.1.2	**Entity's Senior Management reviews and approves all company policies annually.**	**Inspected the company policies to determine that the company policies have been reviewed and approved by the Senior Management.**	**No exceptions noted.**
CC4.1.3	**Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.**	**Inspected that the Senior Management has reviewed and approved the entity's Organizational Structure.** **Evidenced Organization chart.**	**No exceptions noted.**
CC4.1.4	**Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.**	**Inspected the Risk Management Process showing that the Senior Management has reviewed and approved the documents.** **Evidenced Risk register.**	**No exceptions noted.**
CC4.1.5	**Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.**	**Evidenced Risk register.**	**No exceptions noted.**
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1.6	**Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.**	**Inspected Records of Third-Party vendor and service provider assessments to determine that the entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.** **Evidenced Risk register.**	**No exceptions noted.**
CC4.2: COSO Principle 17: 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.			
CC4.2.1	**Entity has provided information to employees, via the Security Incident Management Policy, on how to report failures, incidents, concerns, or other complaints related to**	**Observed Incident reports and Investigation records for security incidents and breaches document that describes how to report incidents to determine that the entity has provided**	**No exceptions noted.**

	the services or systems provided by the Entity in the event there are problems.	information to employees, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	
CC4.2.2	Entity's Senior Management reviews and approves all company policies annually.	Observed that the company policies have been reviewed and approved by Senior Management annually.	No exceptions noted.
CC5.0: CONTROL ACTIVITIES			
CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the Company Procedure & Policies and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.	No exceptions noted.
CC5.1.2	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	Inspected the Acceptable Use Policy to determine that the entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No exceptions noted.
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1.3	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Inspected the Roles & job descriptions document defined by management to determine that the entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	No exceptions noted.
CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			

CC5.2.1	**Entity's Senior Management reviews and approves all company policies annually.**	**Observed that the company policies have been reviewed and approved by Senior Management annually.**	**No exceptions noted.**
CC5.2.2	**Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.**	**Inspected that the Senior Management has reviewed and approved the entity's Organizational Structure.** **Evidenced Organization chart.**	**No exceptions noted.**
CC5.2.3	**Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.**	**Inspected the Risk Management Process showing that the Senior Management has reviewed and approved the documents.** **Evidenced Risk register.**	**No exceptions noted.**
CC5.2.4	**Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.**	**Evidenced Risk register.**	**No exceptions noted.**
CC5.2.5	**Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.**	**Inspected Records of Third-Party vendor and service provider assessments to determine that the entity reviews and evaluates all subservice organizations periodically, to ensure commitments to entity's customers can be met.** **Evidenced Risk register.**	**No exceptions noted.**
CC5.2.6	**Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.**	**Inspected the Company Procedure & Policies and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.**	**No exceptions noted.**

Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	**Entity makes all policies and procedures available to all staff members for their perusal.**	**Inspected the list of policies to determine that the entity makes all policies and procedures available to all staff**	**No exceptions noted.**

		members for their perusal.	
CC5.3.2	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Inspected the Company Procedure & Policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically. Inspected records that the policies have been reviewed and acknowledged by staff members.	No exceptions noted.
CC5.3.3	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Inspected the Company Procedure & Policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding. Observed that the policies have been reviewed and acknowledged by new staff members.	No exceptions noted.
CC5.3.4	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.	Inspected the Company Procedure & Policies and list of policies made available to employees to determine that the entity has developed a set of policies that establish expected behavior with regard to the company's control environment.	No exceptions noted.
CC6.0: 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.			
CC6.1.1	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant	Inspected the Access Management Policy to determine that the entity manages an accompanying process to register and authorize users for issuing system credentials which grant the ability to access	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.2	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inspected the Password Policy to determine that the entity has documented guidelines to manage passwords and secure login mechanisms and make them available to all staff members on the company	No exceptions noted.
CC6.1.3	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected that access to infrastructure assets has been restricted from the public.	No exceptions noted.
CC6.1.4	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those	Inspected that the users of the critical system have been identified and their administrative access has been reviewed by the entity's Senior Management or the Information Security Officer periodically.	No exceptions noted.
CC6.1.5	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected that access to infrastructure assets has been restricted from public internet access.	No exceptions noted.
CC6.1.6	Entity restricts application and software installation as per the policy and procedure defined to manage authorized installations.	Evidenced screenshots of Antivirus status on staff devices.	No exceptions noted.
CC6.1.7	Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected that Role Based Access control to online platforms and company database has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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			
CC6.2.1	**Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.**	**Inspected the Access Management Policy to determine that the entity manages an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.** **Evidenced Access sheet for platforms.**	**No exceptions noted.**
CC6.2.2	**Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.**	**Inspected the Team Member Off-boarding Procedure within HR Policy to determine that the entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.** **Evidenced Human Resources document.**	**No exceptions noted.**
CC6.2.3	**Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.**	**Inspected that Role Based Access control to online platforms and company database has been set up and validated to determine that the entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.**	**No exceptions noted.**
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	**Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on**	**Inspected that Role Based Access control to online platforms and company database has been set up and validated to determine that the**	**No exceptions noted.**

	an individual need or for a predefined role.	entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	
CC6.3.2	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inspected the user access matrix within Access Management Policy where the users of the critical system have been identified and their access to production database has been restricted to only those individuals who require such access to perform their job functions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	Entity has documented policy and procedure to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the Access Management Policy to determine that the entity has documented policy to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	No exceptions noted.
CC6.3.4	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	Inspected the Team Member Off-boarding Procedure within HR Policy to determine that the entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner. Evidenced Human Resources document.	No exceptions noted.
CC6.3.5	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require	Inspected that the users of the critical system have been identified and their administrative access has been reviewed by the entity's Senior Management or the Information Security	No exceptions noted.

	such access to perform their job functions.	Officer periodically. Observed the screenshots of access to critical system.	
CC6.3.6	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected that the users of the critical system have been identified and their access has been reviewed by the entity's Senior Management or the Information Security Officer periodically. Observed the user matrix within Access Management Policy.	No exceptions noted.
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.			
CC6.5.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected Disposing Procedure within Media Sanitization Policy to determine that the entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Where applicable, entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	Observed the malware-protection software within database encryption status document to determine that the entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software. Observed screenshots of database server encryption.	No exceptions noted.
CC6.6.2	Entity requires that all staff members with access to any critical system is protected with a secure login	Observed screenshots of Multifactor Authentication enabled on all critical systems to determine that the entity requires that all	No exceptions noted.

	mechanism such as Multifactor authentication.	staff members with access to any critical system is protected with a secure login mechanism. Evidenced screenshots of Role based authentication.	
CC6.6.3	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected the Endpoint Security Policy to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	No exceptions noted.
CC6.6.4	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	Inspected the Clear desk & clear screen records to determine that the entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	No exceptions noted.
CC6.6.5	Entity has a documented Endpoint Security Procedure and makes it available for all staff on the company intranet.	Inspected the Endpoint Security Policy.	No exceptions noted.
CC6.6.6	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected Access to Critical Systems document to determine that the entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
CC6.6.7	Entity has a documented Password management and makes it available to all staff members on the company intranet.	Inspected Password Policy.	No exceptions noted.
Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.8	Entity develops, documents, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Verified the Hardware inventory within Asset Management Policy to determine that the entity develops, documents, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve	No exceptions noted.

		accountability.	
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.			
CC6.7.1	**Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.**	**Inspected the Endpoint Security Policy to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.**	**No exceptions noted.**
CC6.7.2	**Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.**	**Inspected the Encryption of data at rest within database encryption status document to determine that the entity has set up Encryption mechanisms to encrypt all production database[s] that store customer data at rest.**	**No exceptions noted.**
CC6.7.3	**Entity develops, documents, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.**	**Verified the Hardware inventory within Asset Management Policy to determine that the entity develops, documents, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.**	**No exceptions noted.**
CC6.7.4	**Entity ensures that customer data used in non-production environments requires the same level of protection as the production environment.**	**Inspected the Hardware inventory assets within Asset Management Policy have been identified to determine that the entity ensures that customer data used in non-production environments requires the same level of protection as the production environment.**	**No exceptions noted.**
CC6.7.5	**Entity has a documented policy to manage encryption and cryptographic protection controls.**	**Evidenced screenshot of database server encryption to determine that the entity has a documented policy to manage encryption and cryptographic protection controls.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7.6	Entity restricts application and software installation as per the policy and procedure defined to manage authorized installations.	Evidenced Compliance document to determine that the entity restricts application and software installation as per the policy and procedure defined to manage authorized installations. Evidenced screenshots of Antivirus status on staff devices.	No exceptions noted.
CC6.7.7	Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected Access to Critical Systems to determine that the entity requires that all critical endpoints are encrypted to protect them from unauthorized access.	No exceptions noted.
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.			
CC6.8.1	Entity restricts application and software installation as per the policy and procedure defined to manage authorized installations.	Evidenced screenshots of Antivirus status on staff devices.	No exceptions noted.
CC6.8.2	Entity requires that all employee endpoints be audited periodically to ensure that the Operating System version is current or next most current.	Inspected Endpoint Security Policy to determine that the entity requires that all employee endpoints be audited periodically to ensure that the Operating System version is current or next most current.	No exceptions noted.
CC6.8.3	Entity maintains a record of log management procedure and authorized personnel details.	Evidenced Employee log in and log out records to determine that the entity maintains a record of log management procedure and authorized personnel details.	No exceptions noted.
CC6.8.4	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's	Observed the entity's firewall in the system to determine that every production host is protected by a firewall	No exceptions noted.

	cloud provider.	**with a deny-by-default rule.** **Inspected the Network Security Policy.**	
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.0: 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.			
CC7.1.1	**Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.**	**Inspected Vulnerability and Patch Management Policy to determine that the entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.** **Evidenced Vulnerability assessments and Penetration Testing Report.**	**No exceptions noted.**
CC7.1.2	**Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.**	**Inspected Source Code review Report to determine that the entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.**	**No exceptions noted.**
CC7.1.3	**Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.**	**Inspected the Vulnerability and Patch Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.**	**No exceptions noted.**
CC7.1.4	**Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.**	**Observed threat detection by performing risk assessment to detect anomalous or suspicious activity and threats.** **Inspected Risk Assessment and Risk Treatment Plans document.**	**No exceptions noted.**
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.			

CC7.2.1	**Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.**	**Observed Vulnerability scanning performed to determine that the entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.**	**No exceptions noted.**
CC7.2.2	**Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.**	**Inspected Vulnerability and Patch Management Policy to determine that the entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.** **Evidenced Vulnerability assessments and Penetration Testing Report.**	**No exceptions noted.**

Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.2.3	**Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.**	**Inspected the Vulnerability and Patch Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.**	**No exceptions noted.**
CC7.2.4	**Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.**	**Observed threat detection by performing risk assessment to detect anomalous or suspicious activity and threats.** **Inspected Risk Assessment and Risk Treatment Plans document.**	**No exceptions noted.**
CC7.2.5	**Entity identifies vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third-party service provider.**	**The organization is committed to conducting penetration testing exercise by a qualified third-party service provider to determine that the entity identifies vulnerabilities on the company platform annually.** **Verified the VAPT Report.**	**No exceptions noted.**
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.			

CC7.3.1	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and	Inspected Incident register to determine that the entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy	No exceptions noted.
CC7.3.2	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	Inspected the Vulnerability and Patch Management Policy to determine that the entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No exceptions noted.
CC7.3.3	Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected Vulnerability and Patch Management Policy to determine that the entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities. Evidenced Vulnerability assessments and Penetration Testing Report.	No exceptions noted.
CC7.3.4	Entity identifies vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third-party service provider.	The organization is committed to conducting penetration testing exercise by a qualified third-party service provider to determine that the entity identifies vulnerabilities on the company platform annually. Verified the VAPT Report.	No exceptions noted.
Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3.5	Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Observed threat detection by performing risk assessment to detect anomalous or suspicious activity and threat. Inspected Risk Assessment and Risk Treatment Plans document.	No exceptions noted.
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.			

CC7.4.1	**Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.**	**Inspected the Incident Management Policy to determine that the entity has established a policy and procedure which include guidelines to be undertaken in response to information security incidents.**	**No exceptions noted.**
CC7.4.2	**Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.**	**Inspected Incident register to determine that the entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.** **Verified Incident Reports.**	**No exceptions noted.**
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	**Entity has documented Business Continuity & Disaster Recovery Policies, that establish guidelines and procedures on continuing**	**Inspected the Business Continuity and Disaster Recovery Policy to determine that entity establish guidelines and procedures on continuing**	**No exceptions noted.**
CC7.5.2	**Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.**	**Inspected the Data Backup Policy to determine that the entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.** **Evidenced screenshots of database backup configurations.**	**No exceptions noted.**
CC7.5.3	**Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.**	**Inspected the Business Continuity and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.**	**No exceptions noted.**
Control #	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**

CC8.0: 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.			
CC8.1.1	**Entity develops, documents, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.**	**Verified the Hardware inventory within Asset Management Policy to determine that the entity develops, documents, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.**	**No exceptions noted.**
CC8.1.2	**Entity has documented policies and procedures to manage changes to its operating environment.**	**Inspected the Change Management Policy to determine that the entity has documented procedures to manage changes to its operating environment.**	**No exceptions noted.**
CC8.1.3	**Entity has procedures to govern changes to its operating environment.**	**Inspected the Change Management Policy.**	**No exceptions noted.**
CC8.1.4	**Entity has established procedures for approval when implementing changes to the operating environment.**	**Evidenced change management configuration document.**	**No exceptions noted.**
CC9.0: RISK MITIGATION			
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	**Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements.**	**Inspected Risk Management Process to determine that the entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated by incorporating the entity's service commitments and system requirements.** **Evidenced Risk register.**	**No exceptions noted.**
CC9.1.2	**Entity performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.**	**Inspected the Risk Management Policy.** **Verified the Risk register.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.3	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the Risk Management Process to determine that each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Evidenced Risk register.	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners			
CC9.2.1	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments	Inspected the Risk Management Process to determine that the entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated incorporating	No exceptions noted.
CC9.2.2	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inspected Records of Third-Party vendor and service provider assessments to determine that the entity has a documented policy and procedure to manage Vendors/third-party suppliers and provide	No exceptions noted.
CC9.2.3	Entity has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.	Inspected Records of Third-Party vendor and service provider assessments to determine that the entity has a documented Vendor Management Policy that provides guidance to staff	No exceptions noted.

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.0: ADDITIONAL CRITERIA FOR AVAILABILITY			
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.			
A1.2.1	**Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.**	**Inspected the Data Backup Policy to determine that the entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.** **Evidenced screenshots of database backup configurations.**	**No exceptions noted.**
A1.2.2	**Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.**	**Inspected the Data Backup Policy to determine that the entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verify the integrity of these backups.**	**No exceptions noted.**
A1.2.3	**Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.**	**Inspected the Business Continuity and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.** **Evidenced disaster recovery exercise document.**	**No exceptions noted.**
A1.2.4	**Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.**	**Inspected the Business Continuity Planning within Business Continuity and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.**	**No exceptions noted.**
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	**Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.**	**Inspected the Business Continuity Planning within Business Continuity and Disaster Recovery Policy document to determine that the entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.2	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the Disaster Recovery Procedure within Business Continuity and Disaster Recovery Policy to determine that the entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No exceptions noted.
A1.3.3	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	Inspected the Disaster Recovery Procedure within Business Continuity and Disaster Recovery Policy to determine that the entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.	No exceptions noted.

CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.0: ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	**Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.**	**Inspected the Company Procedure & Policies to determine that the entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.** **Observed that the policies have been reviewed and acknowledged by new staff members.**	**No exceptions noted.**
C1.1.2	**Entity has established procedures for staff to acknowledge applicable company policies periodically.**	**Inspected the Company Procedure & Policies to determine that the entity has established procedures for staff to acknowledge applicable company policies periodically.** **Inspected records that the policies have been reviewed and acknowledged by staff members.**	**No exceptions noted.**
C1.1.3	**Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.**	**Inspected Data Classification Policy to determine that the entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.**	**No exceptions noted.**
C1.1.4	**Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.**	**Inspected the Database Encryption status document to determine that the entity has set up Encryption mechanisms to encrypt all production database[s] that store customer data at rest.**	**No exceptions noted.**
C1.1.5	**Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.**	**Inspected Information Security Policies to determine that the entity has documented policies that govern the confidentiality, integrity, and availability of information systems.**	**No exceptions noted.**
C1.1.6	**Where applicable, entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.**	**Inspected the Endpoint Security Policy to determine that the entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.**	**No exceptions noted.**

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected Media Sanitization Policy and Data Classification Policy to determine that the entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	No exceptions noted.
C1.2.2	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Inspected Media Sanitization Policy to determine that the entity has a documented policy outlining guidelines for the disposal and retention of information.	No exceptions noted.

THANK YOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://www.youtube.com/@SECURECYBERGATES
https://securecybergates.com/services
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com