Introducing THE IP PLATFORM

THE IP PLATFORM is CPA Global’s unified and consolidated view of all global innovation and IP rights information, workflows and tasks through aggregation and integration of various services.

To read more about The IP Platform, please visit www.cpaglobal.com/the-ip-platform

Datacenter Security

THE IP PLATFORM is hosted on Microsoft Azure provided infrastructure and platform services available in United States (US) as a multi-tenant public cloud product. Azure runs on geographically distributed Microsoft facilities, highly clustered, robust and secure hosting environment. Each facility employs various security provisions for perimeter control like barriers, fencing, video surveillance, seismic bracing, intrusion detection and other electronic means. Authorized staff undergo physical screening and two-factor access control: biometric and card readers to access datacentre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Azure datacenters are equipped with fire detection and suppression equipment which utilizes smoke detection sensors across the building and utility areas. The datacentre is also installed with fully redundant, serviceable 24x7 electrical power systems, UPS and generators for multiple days of back-up power, climate control to ensure a consistent operating temperature for hardware, automated monitoring and management of all electrical, mechanical, life support systems and equipment.

To read further on Azure Datacenter Security please read https://www.microsoft.com/en-in/cloud-platform/global-datacenters

<table>
<thead>
<tr>
<th>Azure Regions for THE IP PLATFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America (US)</td>
</tr>
<tr>
<td>• Primary Location - US East</td>
</tr>
<tr>
<td>• Backup Location – US West</td>
</tr>
</tbody>
</table>

THE IP PLATFORM has certain middle tier components deployed in EU-West region.

<table>
<thead>
<tr>
<th>Certifications / Attestations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC:ISO27001</td>
</tr>
<tr>
<td>AICPA SOC2 Type 2</td>
</tr>
</tbody>
</table>

Security Features

THE IP PLATFORM has been designed to offer the performance, scalability, security and service levels that customers can rely upon. CPA Global has utilised state-of-the-art technology and processes to maintain consistent and reliable access, security, and privacy for every customer. THE IP PLATFORM leverages Azure’s built-in capabilities for compliance with a wide range of regulations and privacy mandates. Azure offers huge flexibility and elasticity to overall hosting and operations approach allowing to architect and dynamically scale for surges in demand. Azure allows CPA Global DevOps team to automate deployments, conduct backups and recovery instances, consume services and streamline operations.

THE IP PLATFORM serves multiple apps through a front-end as a multi-tenant product and hosted on Azure in the US region with resilience, recovery and fault tolerance. The key components of THE IP PLATFORM are:

Static Content: THE IP PLATFORM has been built as a SPA (Single Page Application). All necessary code (HTML, JavaScript, and CSS) is retrieved with a single page load from the ‘Static Content’ component, which is hosted as a separate sub-domain.

CPA GLOBAL®
**Dynamic Content**: The SPA loads all data from the ‘Dynamic Content’ component which is also hosted as a separate sub-domain. The Dynamic Content is delivered using Web API 2.x, which basically are REST endpoints implemented on Microsoft .NET framework.

**Database**: The core functionality within THE IP PLATFORM and some of the services division require relational database to store data. It includes row level security, groups, group hierarchies, group memberships, settings, profiles etc. For services division it would store portfolio data, categorisations and, in the case of File History, order data, and alert services.

**Single Sign-On (SSO)**: The SSO feature provides THE IP PLATFORM customers the ease to sign in all of CPA’s applications using a single account. This means that customers can log-in once and can access the applications without logging-in to each application individually. Each customer on THE IP PLATFORM will be either federated through an ID provider that is available at the customer’s organisation (like ADFS) or through a customer account that is available within the CPA Cloud Directory.

**Identity Access Management (IAM) and Access & Group Management (AGM)**: Identity and Access Management (IAM) is CPA Cloud Directory that acts as an ID provider for the customers who do not have another ID provider to federate with an SSO solution. Access and Group Management (AGM) solution provides centralised access control for multiple CPA applications. It supports sub-organisations that may extend SSO to customer organisations.

**Backend Services**: These are services used to handle indexing of data, synchronisation, integration with external resources etc. These services are hosted as Windows Services using the same solution as described under Dynamic Content, where components are dynamically loaded.

---

**Host Security**

THE IP PLATFORM is designed and built as a cloud native product leveraging Azure’s Platform-as-a-Services (PaaS) components and has a very limited use of virtual servers. All hosts and service endpoints in Azure are deployed with highest levels of security like use of Azure provided images of Windows Server, running Azure Web Apps within App Service Environments (ASE), Encrypted storage volumes & blobs, consuming Azure SQLaS database service enabled for encryption at rest, network isolation and assign resource-level permissions. Virtual hosts are hardened and undergo regular patching cycles, also installed with Anti-Virus, Anti-Malware and File Integrity Monitoring.

**Environment Segregation**

Production and Development/QA environments are segregated in separate Azure Subscriptions and individual Azure Virtual Network (VNET) to prevent unauthorized access or changes to information assets. Azure networks are segregated at network level using VNET and network access is governed through Access Control Lists (ACL) on virtual firewalls. Microsoft Azure Active Directory (AD) and the CPA Global-hosted Active Directory is used to identify and access management for THE IP PLATFORM that helps secure access to customer data and simplifies the management of users and groups. It combines core directory services, identity governance, security, and application access management. Active Directory is used to build policy-based identity management into entire platforms. Additionally, procedures are in place to ensure production data is not used in nonproduction environments.

**Data Segregation**

THE IP PLATFORM is a multi-tenant SaaS product and client data within the apps are a schema level logical segregation within the database and storage blobs. The access to data is governed by access keys, row level security, groups, and group memberships.
**Network Security**

All production instances and non-production environments are secured through a multi-layered security topology with Layer 3 and Layer 7 firewalls, Load Balancers, Intrusion Prevention and Denial of Service (DoS) protection. Traffic flow policies are enforced through ACLs on each managed interface up to the level of hosts and endpoints. Any changes to network rules or configuration are subject to a formal change approval from security team. The load balancers are also configured to support end-to-end traffic encryption using Transport Layer Security (TLS).

Azure environment leverages Network Security Groups, Subnets and Route tables in VNET to implement a complete firewall solution enabling traffic filtering by protocol, service port and source/destination IP. Traditional Layer 2 security attacks, including MAC spoofing and ARP spoofing, are blocked by default. Azure environment also has protection against Distributed Denial of Service (DDoS) to prevent network and transport layer attacks.

**User Access Management**

The SSO feature provides clients a secured mechanism to sign-in into all THE IP PLATFORM apps using a single account. This means that customers can log-in once and can access the applications without logging-in to each application individually. Each client on THE IP PLATFORM will be either federated through an ID provider that is available at the client’s organisation (like ADFS) or through a customer account that is available within the CPA Cloud Directory.

Each client administrator can configure role-based and context-based entitlements while granting access to data within the app unless managed by CPA Global’s software support teams on behalf of clients. Clients are responsible for keeping passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable.

**Privileged Access Management**

The Information Security Policy at CPA Global requires that access to information assets to be granted based on business justification, with the appropriate authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.

THE IP PLATFORM has been implemented in Azure with well-defined, fine-grained roles and access into cloud hosted systems through Azure Identity and Access Management (IAM) tool. The Azure AD is configured to only use CPA Global’s Active Directory Federation Services (ADFS) for authenticating into Azure hosted systems and is configured to use Multi Factor Authentication (MFA).

All Controls are implemented for segregation of duties, role-based access and access to resources is granted on the principle of least privilege. Logging and monitoring of privileged access to information security management systems is enforced in accordance with CPA Global Log Management and Monitoring Policy, reviewed on regular basis.

**Encryption & Key Management**

Industry-standard encryption protocols and ciphers are used to enable encryption for data in transit and at rest on Azure. TLS v1.1 and higher is implemented with key exchange algorithm that supports perfect forward secrecy and provides encryption of 128 bits or stronger. Encryption at Rest is enabled across the board for all data and databases, including logs using Transparent Disk Encryption (TDE) on Azure SQLaS and compute instances with Azure encryption.

CPA Global has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission. Azure instance leverages Azure Key Vault which uses Hardware Security Module (HSM) to generate, store & manage all cryptographic keys for data encryption, designed to securely store and process cryptographic key material for a wide variety of uses such as database encryption, Public Key Infrastructure (PKI), authentication and authorization.

**Capacity Management**

Proactive monitoring across the full stack in Azure continuously measures the performance of key subsystems of the product against the established boundaries for acceptable service performance and availability. Upon breach of any thresholds or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. System performance and capacity utilization is proactively planned to optimize the environment.
**Logging & Monitoring**

**THE IP PLATFORM** leverages Azure’s diagnostic and audit log feature which generates extensive logging. The diagnostic and audit logs of **THE IP PLATFORM** resources are sent to the Azure storage account.

Logs of **THE IP PLATFORM** are stored encrypted using Azure SSE utilising 256-bit AES encryption. The logs stored in the Azure storage account.

Real-time threat monitoring and analysis is performed for the detection of anomalous activity within the network, systems, service components and users by CPA Global’s Security Monitoring Cyber Security Team. Threat analytics are used for behaviour analysis of the users, devices and heuristics to detect suspicious activity that indicate a threat and notifications sent in real-time.


**Resilience and Recovery**

**THE IP PLATFORM** leverage Azure provided infrastructure services and product capabilities to implement a warm standby solution, preferring horizontal scaling over vertical scaling. The term warm standby is used to describe a Disaster Recovery scenario in which a scaled-down version of a fully functional environment is always running in the cloud. In the event of a disaster scenario, the system is scaled up quickly to handle the production load. In Azure, this can be done using load balancer, App Service Environment (ASE) and elastic databases.

**THE IP PLATFORM** is designed to provide durability and reliability for customer data. Data is protected by locally redundant storage and geo-replication, which is used to maintain multiple replicas of data within a single region and also provides redundancy of data across regions to ensure redundancy.

**RTO and RPO**

- **Azure Environment**
  - Recovery Time Objective (RTO) of 4 Hours.
  - Recovery Point Objective (RPO) of 15 Minutes for data loss.
  - Backup Retention period of 5 Years.

Disaster Recovery test is conducted annually, and a real-time simulation test would include the following steps -

Phase 1: Disaster Recovery Launch Authorization phase - to detect service disruption or outage, determine recoverability and the extent of the damage to activate the plan.

Phase 2: Recovery phase - to break replication services, restore services and make network/URL changes

Phase 3: Reconstitution phase - to restore processing capabilities and resume/rebuild services for primary environment.


To read further on Azure regions, please read [https://azure.microsoft.com/en-in/regions/](https://azure.microsoft.com/en-in/regions/)
THANK YOU