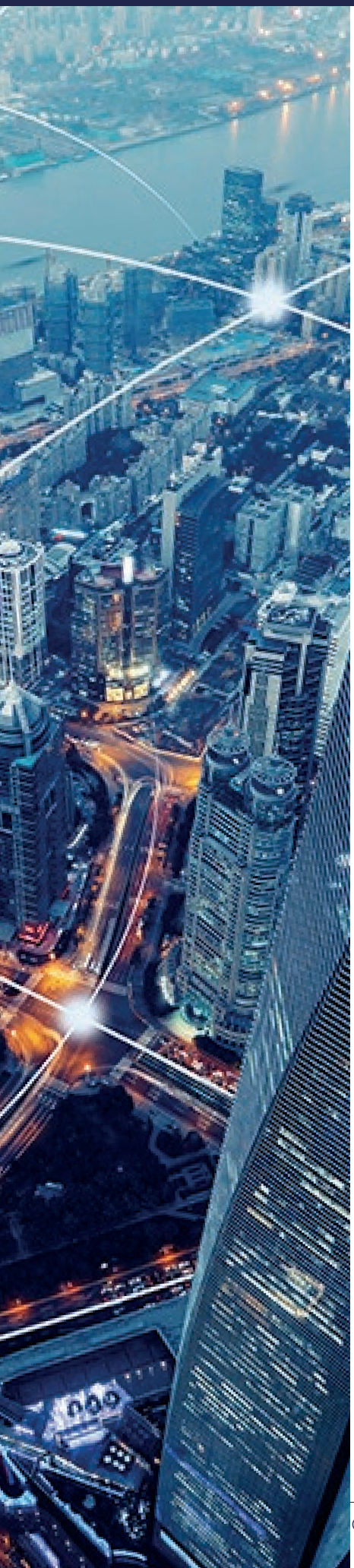
INFORMATION SECURITY & PRIVACY WHITEPAPER

ivalua

ALL Spend, ALL Suppliers, NO Compromises



Introduction

All aspects of business are becoming increasingly digital. In that landscape, it is of paramount importance to secure our customer's business and intellectual property. In addition, while organizations are facing more and more sophisticated threats, it is critical for SaaS providers to deliver security across all aspects of service.

Ivalua provides a cloud-based spend management platform that empowers customers to effectively manage all their spend and suppliers, reducing costs, mitigating risk, improving employee productivity/ satisfaction, accelerating innovation and delivering a range of other benefits. As an essential part of the enterprise IT architecture for many of the world's most demanding and admired brands, Ivalua is dedicated to ensuring the highest levels of security to our customers. We pride ourselves on eliminating the typical compromises organizations accept with Spend Management solutions. One of these is between the convenience and low total cost of ownership of cloud-based solutions and robust security. Ivalua's platform offers both.

This white paper describes Ivalua's security program across several key security domains. All these domains are represented from the context of Ivalua as a Software as a Service (SaaS) provider.

This whitepaper is provided for informational purpose only and does not create a contractual commitment or legal advice.

Architecture

The Ivalua cloud features a “multi-instance” architecture that delivers logical single tenancy by isolating all customers’ data from each other. This is achieved by utilizing an enterprise grade cloud architecture and a dedicated database and application set per customer instance.

The logical architecture of Ivalua’s platform is described below:

Customers and web services connect to the Ivalua cloud over HTTPS, using TLS for communication to and from an Ivalua instance. All interactive end-user activities are performed using a standard Microsoft, Firefox or Chrome web browser. There is no requirement for customers to install any client software on any desktop, laptop, tablet, or smart phone in order to access their Ivalua instances.

Database Architecture

The database layer consists of database servers, installed in a discrete, non-internet routable network segment. Requests from end-users or integrations cannot be made directly to the database tier and are only issued from a customer’s Ivalua instance.

Each application instance has a single database present on a database server running multiple discrete databases. There is no commingling of any customer data between application instances and databases, nor shared multi-tenant databases with data from multiple customers stored therein.

Ivalua’s customers benefit from multiple layers of robust separation, rather than a single logical control.

Application Architecture

Application servers are in a discrete network segment. These servers host application nodes for each customer’s Ivalua instance and are the termination point for all inbound requests made by end-users of those instances. Requests are received by the relevant application nodes and processed by them, including being appropriately escaped or encoded as required, before passing to the relevant database service in the database server tier.

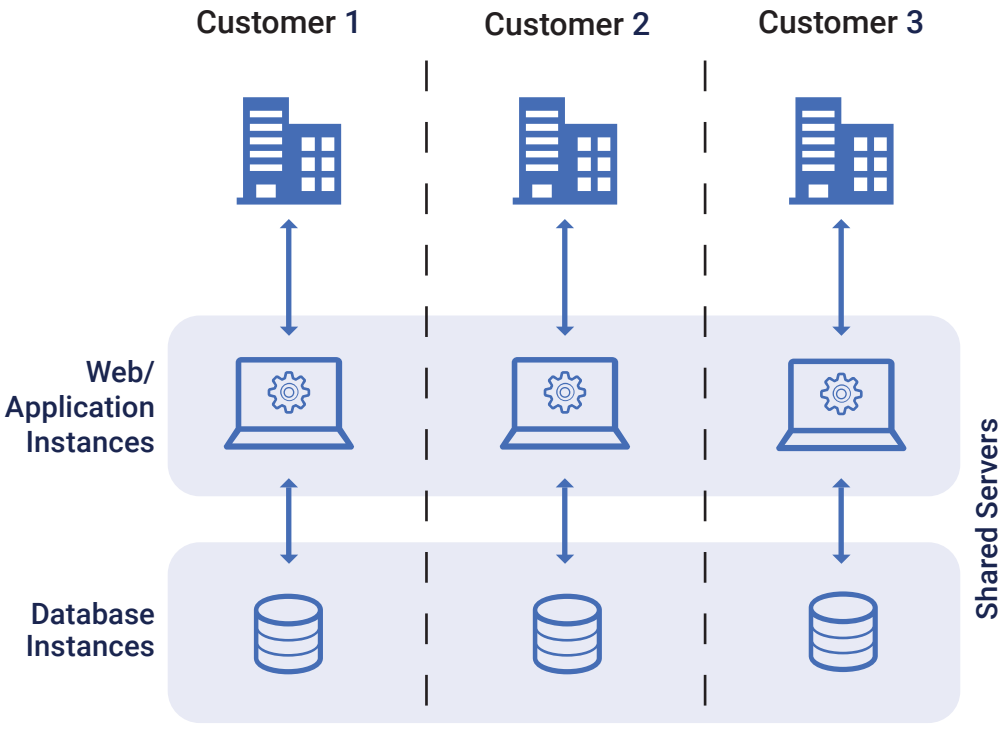


Figure 1: Ivalua’s Single tenant - multi-instance architecture

Security Advantage of Using Ivalua's Multi-instance Architecture.

Ivalua's Multi-instance SaaS	Multi-tenant SaaS
Customer's data is separated from any other customer at multiple layers, minimizing the chance of one customer accessing another customer's data intentionally or accidentally.	Walls between data of different customers are much thinner - tagging and access control mechanisms are generally used to segregate data. Using such techniques have the potential for misalignment of data or records to incorrect owners. Defects, faults, or weaknesses in access control list processing could also potentially lead to data leakage.
Built in security of database can be leveraged to prevent and discourage hacking.	Will need to develop their own systems to achieve these same benefits.
A penetration attack is isolated to the single customer, and doesn't impact other customer.	A penetration attack on a single customer exposes all customer of the SaaS. Both data access and performance can be impacted.
Customers can perform their own scanning and penetration testing to self-assess the security of the Ivalua application.	Generally, customers are not allowed to perform penetration testing, as it risks exposing other customers' data and impacting system performance.
Customer can request Disaster Recovery (DR) failover for their own application and database at anytime.	Customer has to rely on the SaaS provider for a DR test and even in that scenario, the DR test is not always specific of their instance.
Flexibility in meeting customers' data privacy and additional data isolation (dedicated virtual or physical servers) requirements.	Limited hosting flexibility or prohibitive costs associated with data isolation.

Other Benefits of Using Ivalua's Multi-instance Architecture.

Ivalua's Multi-instance SaaS	Multi-tenant SaaS
Customers can choose the timing for the application upgrade per their schedule.	Customers are forced to accept software updates and are dependent on the SaaS provider upgrade timeline.
Agile and flexible way to support customer's business need of having multiple application instances.	Requesting and provisioning a new application instance is generally a time consuming effort.
Solution can be customized to meet business needs.	Same standard application for all customers.

Information Security Governance and Risk Management

Security Frameworks & Policies

Ivalua's security framework is based on NIST 800-53 and ISO/IEC 27001:2013. Ivalua's security program is expressed through its Information Security policy, standards, plans and in an extensive library of standard operating procedures (SOPs) and other relevant documentation and guidance. The policy, standards, plans and SOPs are periodically reviewed and updated.

Security Management

The security program at Ivalua is led by its Chief Information Security Officer (CISO), who is part of the Executive Team and closely coordinates the Infosec program along with the CEO, CTO, CPO and other executives. This organizational structure provides visibility and oversight with respect to security programs.

The CISO is supported by a dedicated security team and a number of specialists across the IT and R&D teams. These include architects, security engineers, operations, application security, and governance, risk and compliance specialists. This team liaises with customers on security matters and implements security and privacy controls internally within the organization.

Risk Management

Ivalua has a defined process for managing information security risks. Regular assessments are performed in order to identify security risks and assess likelihood and impact related to such risks. Ivalua manages risks identified in an effective and timely manner to safeguard Ivalua's customer data and to ensure minimal disruption to its service.

Privacy

Ivalua's application implements privacy by design to help support our customers' privacy compliance requirements. Ivalua's customers are responsible for determining the collection, storage, usage, sharing, archiving, and destruction of data processed in their Ivalua instances. As the data controller, Ivalua's customers are responsible for meeting the requirements of relevant privacy legislation in the jurisdiction in which they operate and from which they collect personal data. Ivalua has no visibility or understanding of the conditions under which the data was collected, if appropriate permission was obtained, or whether it is being used in accordance with those conditions.

Ivalua is committed to protecting the confidentiality of any data its customers entrust to it.

Customer data remains the exclusive property of the customer at all times. For example, if and when a third party requests to change said data, Ivalua will always refer that individual to the customer who owns the data.

The General Data Protection Regulation (GDPR)

Ivalua fulfills the role of the data processor under GDPR and complies with its obligations. Ivalua has implemented numerous privacy and security practices to ensure Ivalua compliance with the GDPR. These practices include:

- Training personnel on privacy and security practices, including privacy by design principles.
- Conducting privacy impact assessments.
- Providing highly configurable features to our customers to also enable them to manage their obligations (access controls, anonymization methods, etc.).
- Maintaining records of processing activities.

Cross-Border Data Transfers

Strict data protection laws govern the transfer of personal data from the European Economic Union to countries without an adequate level of protection comparable to the statutory level of data protection with the European Economic Area (EEA). To address this requirement, Ivalua has incorporated the European Commission's approved standard contractual clauses, also referred to as the "Model Contract" into its standard form of Data Protection Agreement. The Model Contract creates a contractual mechanism to meet the adequacy requirement to allow transfer of personal data outside the EEA. In addition, Ivalua has instituted a written data transfer agreement between each of its group companies (i.e., Ivalua legal entities in the United States, the EEA and elsewhere) to ensure the legal protection of data transfers between our global affiliated companies.

Regulatory & Industry Compliance and Certifications

Ivalua has a dedicated governance, risk, and compliance (GRC) team responsible for managing Ivalua's security compliance program. This team engages across multiple functional areas within Ivalua, including legal, HR, marketing, R&D and IT to manage the compliance program. Ivalua's legal organization maintains a current understanding of obligations to existing and new laws and statutory regulations within the jurisdiction in which it operates.

Ivalua currently maintains the following certifications to support its customers compliance obligations:

Certification	Geography	Industry or Vertical or Geography	Third Party Audited/ Attested
SOC 2 Type 2	International	All	Annually
SSAE 18 SOC 1 Type 2 ISAE 3402	International	All	Annually
HIPAA/HITECH	US	US - Healthcare	Annually

Physical Security & Architecture

Ivalua co-locates its production system in state-of-the-art data centers or IaaS providers designed to host most-critical computer systems with fully redundant subsystems and compartmentalized security zones. Currently nine(9) data center/IaaS providers exist across four (4) geographic regions. Ivalua data centers/IaaS providers adhere to the strictest physical security and environmental control measures. Our data center/IaaS partners adhere all to the stringent data center certifications: ISO 9001/14001/ISO 27001/SOC I and II.

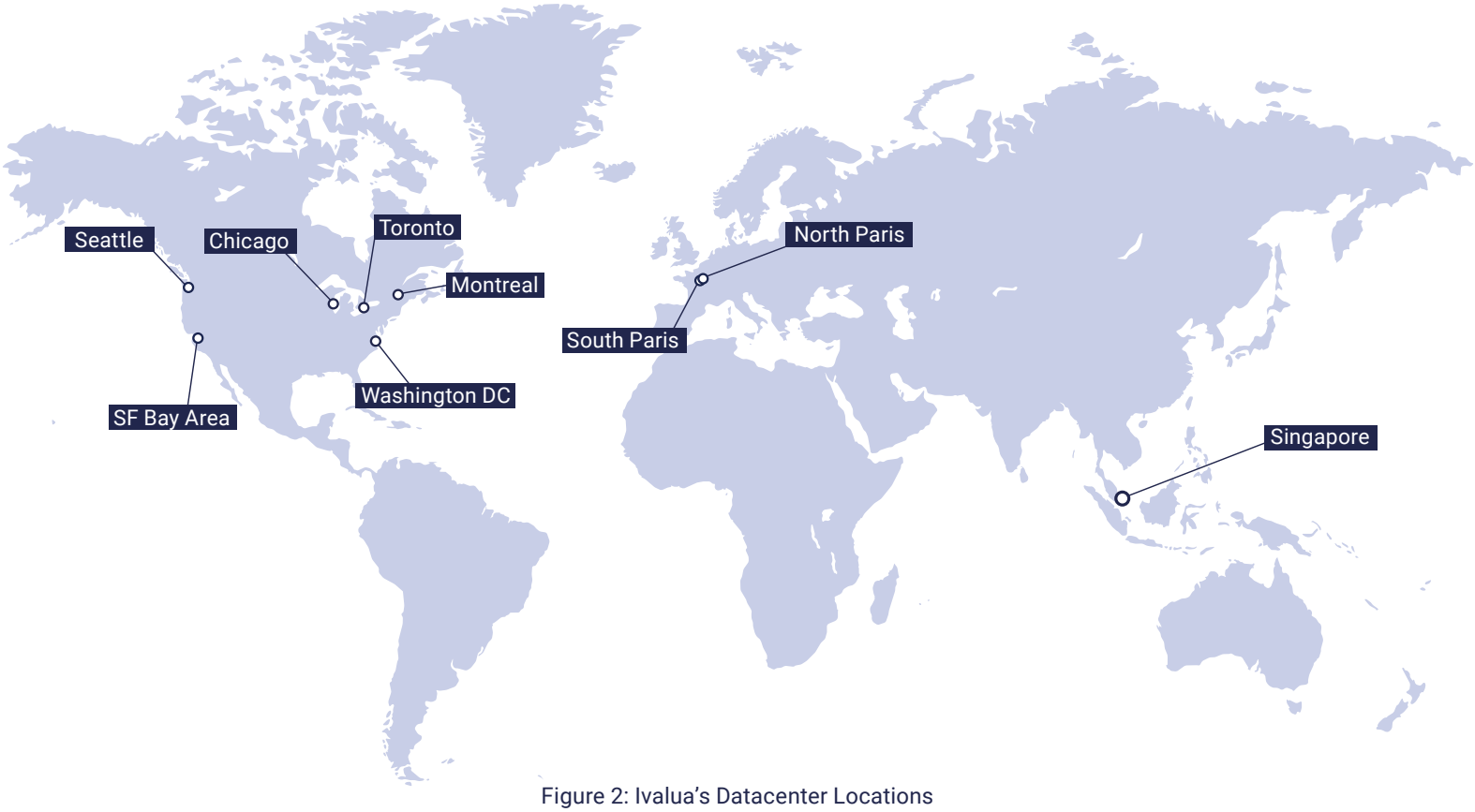


Figure 2: Ivalua's Datacenter Locations

The datacenter providers have no logical access to any Ivalua's systems or customer data and solely provide private colocation spaces and environmental resources. Physical access to the data centers is highly restricted and stringently regulated. Ivalua operations use best practices such as "least access" hardened servers and regularly scheduled maintenance windows

Human Resource Security

At initial stages of the employment process for prospective candidates, Ivalua undertakes background checks and all roles, subject to local laws and restrictions. The background checks includes checks for criminal, employment, financial, citizen status, and government watch lists. Failure to pass these tests will result in either mandatory disqualification from the employment process or a further follow up investigation.

As a condition of accepting employment, Ivalua personnel are required to sign a non-disclosure agreement, and review and confirm their understanding of Acceptable Use Policy. This confirmation is recorded electronically.

Personnel are also required to undergo annual security and compliance training and fulfillment of training requirements is measured and enforced. The content of the training varies from year to year, as different security topics, risks, threats and requirements are identified.

Data Security

Data Segregation

Ivalua is a multi-instance SaaS application and this allows us to provide our customers a complete separation of their data from other customers not only at the database level, but also application server level. Isolating customers' data creates an additional barrier to prying eyes

Encryption of Data at Rest

When the customer chooses to deploy Ivalua's HSM encryption offering, Ivalua encrypts customer data at rest in the database with no impact to functionality. It utilizes the native capabilities of the database engine to encrypt data as it is written to the database and decrypt as it is read from the database using industry standard Advanced Encryption Standard (AES) algorithm with a key size of 256 bits. This technology, often called Tablespace Encryption or Transparent Data Encryption (TDE), is fully transparent to the customer and to the application.

When using Database Encryption all data is encrypted, including attachments, logs, and backups. File attachments are encrypted by the application prior to being saved to disk, and only decrypted on the fly when requested back.

Full disk encryption is provided via self-encrypting hard drives with AES-256 bit encryption. This delivers "at-rest" protection focused on preventing data exposure through the loss or theft of hard disks holding customer data. Using the full disk encryption does not impact the performance or functionality of the application.

Portable devices such as laptops are encrypted by a full disk encryption with pre-boot authentication.

Encryption of Data in Transit

The web traffic between the end-users and the servers is encrypted using TLS (HTTPS) up to AES-256 depending on the user's browser cypher suite support. Ivalua SSL X.509 CA certificates are generated with RSA 2048 key size and SHA-256. This secures network traffic from passive eavesdropping, man-in-the-middle attacks, active tampering and forgery of messages.

Encryption Key Management

Encryption keys are managed with utmost care by the IT Department. Encryption keys for the database, files and backups are unique per customer tenancy. Encryption keys are generated and stored using highly secure FIPS 140-2 level 2 or higher modules, backed up regularly and are revoked at the end of the crypto-period. In a scenario of key compromise (note: we haven't had such an incident), we will revoke the encryption keys and not use such a key again. Access to the encryption key is highly restricted to a fewest number of custodians necessary.

Data Management

Data Classification

Ivalua applies a single data classification to all customer data it hosts. Ivalua does not inspect or monitor its customers' data and has no ability to understand how any data may have been classified by individual customers. Ivalua treats and handles all customer data the same way and in accordance with its policies for customer data management.

Customers remain the data owner and data controller of all data they place into their Ivalua instance, and should apply access controls to restrict access to data within their instances based on their own requirements and needs, in accordance with their access control, data retention and data classification policies.

Data Retention

Customers decide what information is to be stored, how it is to be used, and how long it is retained within the Ivalua SaaS application. Ivalua does not delete or modify customer data, and only processes data in accordance with its contractual obligations and the customer's configuration of their instance(s).

Media Disposal

Ivalua uses solid-state or mechanical disks within its colocation spaces. No tapes or other forms of removable media are used in providing the service, including for backups. When functional storage devices are retired, Ivalua decomissions disk storage using a secure wipe protocol commensurate with US Department of Defense standards.

Failed drives/disks are securely stored within the same colocation space where they were formerly used. The drives/disks are zeroed out and then physically shredded using a destruction process that is tracked and recorded.

Data Return and Destruction

Through the term of the contract, customers also have the ability to directly export data using the Query extraction tool available within the Ivalua application. Customers can also request Ivalua to assist with the data extraction. Upon termination of the contract, client data is securely destroyed.

Upon contract expiration or exit, when requested, Ivalua will supply a customer's data in standard txt file format. Customers have 30 days to request their data to be returned, after which all hosted and its backed-up data is automatically deleted and overwritten. The data in the archive is retained until the disk/drives are destroyed or overwritten per Ivalua's disk/drive rotation process.

Network and Operational Security

Network Security

Ivalua has also implemented proactive security procedures, such as perimeter defense and network intrusion prevention systems to secure its perimeter. Dedicated DMZ, network segmentation, dedicated URLs and Site-to-Site VPN (note: a paid service) are some of the other measures implemented to protect customer instances from cyber attacks.

Operating System Security

Ivalua builds and maintains standard secure operating system build configurations. Anti-malware measures with regular updates are made to all servers, as well as all Ivalua corporate IT systems and endpoints.

Vulnerability scans (at least monthly) and penetration testing (annually) of the Ivalua infrastructure are also evaluated and conducted on a regular basis by both Internal Ivalua resources and external Third-Party vendors. Patching of affected systems, services, or applications is undertaken promptly (at least monthly), in accordance with Ivalua criteria and processes.

Availability

Data Backups

For clients subscribing to DRP services, the Ivalua primary production database is replicated to a secondary database maintained at an off-site datacenter. Database and transaction logs backups are collected so that a database can be recovered with the loss of as few committed transactions as is commercially practicable.

A full backup is taken from the primary database every week and at least one differential per day. Database backups are retained online for 2 weeks and are then archived for 3 years or as long as necessary to support the interfacing systems (note: this period will vary by system). All backups are written to disk and no tape or removable media is used. Backups of the customer database are encrypted.

The Ivalua backup architecture is not intended to provide archival records. Customers may retain data within their instance for as long as they require in accordance with their policy or regulatory requirements (note: subject to the storage limit or paid service).

Disaster Recovery

Ivalua's Disaster Recovery Plan (DRP) covers its cloud data center environment. Its scope includes all customer instances including those Ivalua systems that are used internally to support the cloud data center. Ivalua warrants its service to its service level agreement (SLA). The SLA includes a disaster recovery (DR) plan for the Ivalua production service with a minimum recovery time objective (RTO) of 4 hours and a minimum recovery point objective (RPO) of 12 hours. The RTO is measured from the time Ivalua production service become unavailable until it is available again. The RPO is measured from the time the first transaction is lost until the Ivalua production services become unavailable.

To make sure Ivalua maintains these SLA commitments, Ivalua maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Ivalua executes its DR plan. The DR plan is tested annually.

Business Continuity

Ivalua's Business Continuity (BC) covers its business functions. The BC Plan (BCP) includes an ongoing Business Impact Assessment (BIA) to understand the impact of the loss of any given system, service, location or function that is required to provide continued support and service to Ivalua's customers.

Authentication and Authorization

A Ivalua application supports multiple form of strong authentication and role-based authorization methods. Ivalua allows customers with ability to set up different authentication requirements for different user populations (e.g. suppliers and internal users)

Single Sign-on Support

While LDAP allows for a unified username/password solution, SAML takes the next step by enabling an enterprise SSO environment. SAML allows for a seamless SSO experience between the customer's internal identity and access management (IAM) solution and Ivalua. Ivalua Solution supports SAML 2.0 protocols for Single Sign On. The Ivalua Solution has been integrated with the most popular Identity providers.

Ivalua Native Login

For customers who wish to use the native login, Ivalua stores their Ivalua password only in the form of a secure hash (salted SHA-512). Unsuccessful login attempts as well as successful login/logout activities are logged for audit purposes. Inactive user sessions can be customer-configured to automatically time-out after a specified time. Customer-configurable passwords rules include length, complexity, number of unsuccessful login attempts and expiration.

Two (2) Factor Authentication

With 2-factor authentication, your account is protected with something you know (your password) and something you have (your phone). Ivalua Solution implements the Time-based One-time Password (TOTP) protocol. 2-factor authentication can be enabled as a required method of authentication for suppliers or for buyers independently.

Authorization

The Ivalua application enforces group policy-based security for authorization. The application prevents any user from directly accessing the production database. Ivalua delivered and customer created profiles, combined with predefined security policies, grant or restrict user access to functionality, business processes, reports, and data whether accessed online or through web services.

Customer configurable profiles are based on users, roles, jobs, organizations location hierarchy, or business sites. System to system access is defined by integration system profiles. Customers can tailor these profiles to meet their needs, providing as fine-grained access as required to support complex configurations, including global implementations.

Software Security

Application Security Testing

Ivalua uses a development process that includes independent validation of the software by a software quality team. Application security testing occurs throughout the software development life cycle. Commercial and in-house tools are used to perform dynamic security testing and static code analysis. Manual testing and code reviews are also performed. All validated critical and high risk security issues are remediated in all supported versions in accordance with Ivalua's policies.

Application Penetration Testing

An external penetration testing is performed on all major releases, prior to the application being made available to the customers. The external penetration testing provides independent review and transparency around Ivalua's secure development practices.

Customer Instance Penetration Testing

Another significant and distinct aspect of Ivalua's application penetration testing is the tests performed by its customers. Unlike other SaaS vendors, our "multi-instance" single tenant architecture makes it possible for customers to perform their own penetration testing on their Ivalua instance. Such testing is allowed only after the customer agrees to the "Rules of Engagement". Scheduling of testing must be pre-approved and conducted at a date and time agreed with Ivalua, to allow Ivalua to monitor activities and be able to differentiate potential attacks from authorized customer testing. Confirmed critical and high-risk vulnerabilities discovered by this process are remediated in accordance with Ivalua's vulnerability management process and criteria.

Security Logging and Monitoring

Ivalua Customer Application Logs

The Ivalua customer application instance generates detailed log and audit information. While a user is logged on, all actions and activities are registered, logged and time-stamped. Every transaction created, every status change, every movement through to the next step in a workflow, every addition or deletion of a data item of any kind can be logged when such activity logs are enabled by the customer. As a result, the system can produce a detailed audit trail of exactly who changed what, where and when. This audit trail can be produced in reports on a real-time basis.

Log information is stored, like all customer data, within tables in a customer's instance. Since the logs when enabled generate a large amount of data, Ivalua only retains the application log data for a rolling 90 day period within the application and in archive for a period of one(1) year. Customers have the ability to forward logs and events to their own logging system or SIEM environment.

Infrastructure Logs

For the purposes of customer security, Ivalua collects and retains logs and events relevant to its cloud infrastructure. It also collects information on requests made to instances on the Ivalua platform in order to detect potentially malicious actions or activities in relation to its service. This information is not available to customers within their Ivalua instances.

Events that occur within a customer instance are accessible to that customer in their instance logs. Events that happen to a customer instance are captured in Ivalua's infrastructure logs.

This white paper is provided for informational purpose only and does not create a contractual commitment or legal advice.

About Ivalua

Ivalua is a leading provider of cloud-based Spend Management solutions. Our complete, unified platform empowers businesses to effectively manage all categories of spend and all suppliers, increasing profitability, lowering risk and improving employee productivity. Trusted by hundreds of the world's most admired brands and recognized as a leader by Gartner and other analysts, Ivalua maintains the industry's leading 98%+ customer retention rate.

Realize the possibilities at www.ivalua.com
Follow us at @Ivalua