Contents
Introduction .................................................................................................................................................. 4
Information Builders and AWS .................................................................................................................. 4
Information Builders Cloud Offerings ....................................................................................................... 4
Description of Services .................................................................................................................................. 5
Understanding the Information Builders Cloud Architecture ....................................................................... 7
Provisioning Options .................................................................................................................................... 7
Network Requirements and Considerations ............................................................................................. 9
Strategy for AWS Accounts ..................................................................................................................... 10
Customer Use Case Sample Architecture ............................................................................................... 10
Information Builders Cloud Security ........................................................................................................... 12
Single Sign On and Identity Management ............................................................................................... 12
Data Privacy: GDPR and CCPA Compliance ............................................................................................. 14
Information Builders Cloud Onboarding Process ........................................................................................ 14
Provisioning New Information Builders Cloud Customers ...................................................................... 16
Roles and Responsibilities ........................................................................................................................... 19
Application Lifecycle Responsibilities ........................................................................................................ 20
Operations: Networking .......................................................................................................................... 20
Operations: AWS RDS Management ....................................................................................................... 20
Operations: Provisioning .......................................................................................................................... 21
Operations: Logging, Monitoring, and Event Management ....................................................................... 21
Operations: Incident Management ........................................................................................................ 22
Operations: Problem Management ......................................................................................................... 22
Operations: Security Management ........................................................................................................... 22
Operations: Patch Management ................................................................................................................ 23
Operations: Continuity Management ....................................................................................................... 23
Operations: Service Request Management ............................................................................................. 23
Information Builders Cloud Support Process .............................................................................................. 24
Appendix A, Foundational Terminology ..................................................................................................... 25
Appendix B, Information Builders Cloud Site-to-Site VPN Information Collection Form ........................... 27
Prerequisites ........................................................................................................................................... 27
Customer VPN Information .................................................................................................................... 27
Introduction

Welcome to Information Builders Cloud! The goal of this document is to provide information about, and assistance with, the Information Builders Cloud Managed Services onboarding process, including a description of available services, roles and responsibilities, and security policies. This document is intended for IT administrators tasked with preparing for and carrying out the tasks required to onboard Information Builders Cloud Managed Services to a new account. The Information Builders Cloud offering includes Information Builders Omni-Gen and WebFOCUS products, Amazon Web Services® (AWS®) Cloud usage and Cloud Managed Services—all in a single integrated stack.

Information Builders and AWS

Information Builders is an Advanced Technology Partner in the AWS Partner Network (APN) and one of the first independent software vendors to subscribe to AWS Managed Services (AMS). The scalability, security, usability, and governance of our award-winning platform align seamlessly with the power and flexibility of AWS. Additionally, our platform supports many of the services available on AWS, including EC2®, S3, Athena, Redshift®, and Relational Database Services. The result is an on-demand, enterprise-scale platform for analytics and data management in the cloud.

Information Builders Cloud Offerings

Information Builders currently provides the following cloud offerings:

- **WebFOCUS Total Access Cloud**
  
  Delivers an all-in BI and analytics platform with end-to-end cloud managed hosting services and cloud support services. All the features and components of WebFOCUS are turned on and available for use with App Studio, Esri®, Hyperstage, and iWay DataMigrator.

- **Omni-Gen™ Total Access Cloud**
  

  - **Omni-Gen™ Integration Edition**
    
    Enables the development, execution, and governance of integration flows linking on-premises and cloud-based processes, services, applications, and data structures, allowing users to access, profile, and integrate data regardless of latency requirements or source type.

  - **Omni-Gen™ Data Quality Edition**
    
    Enables data integration and cleansing technologies to ensure data accessibility, consistency, accuracy, and timeliness.
• **Omni-Gen™ Master Data Management Edition**

Combines data mastering and business-user collaboration to give a 360-degree view of your business.

• **Omni-HealthData™**

Offers a complete information management solution that gives providers and payers a 360 degree view of members, patients, workforce, facilities, community care organizations and other critical domains.

• **Omni-Gen™ for Customer**

Information from assorted systems, external lists, cloud, and on-premises data is consolidated into a single, 360-degree view of every customer.

• **Omni-Gen™ for Supplier**

Information from assorted systems, external lists, cloud, and on-premises data is consolidated into a single, 360 degree view of every supplier.

• **Omni-Insurance™**

Built on the Omni-Gen™ data management platform, Omni-Insurance integrates data from a wide range of internal systems, including claims, billing, policy, rating, human resources, and financial solutions, as well as external data. In addition to providing a subject-oriented data repository that manages mastered subjects and transactional subjects, Omni-Insurance provides business-ready data with a unified, historical view of the book of business.

• **Information Builders Cloud Enterprise**

Specific configurations of our BI and data management offerings are available as AWS-based cloud solutions, via monthly subscription price models. This approach lets you select the software components you require, and your preferred configuration for the AWS cloud (for example, number of cores, Windows®/Linux®, and so on).

**Description of Services**

Information Builders Cloud Managed Services manages operations of your AWS-based Information Builders Cloud infrastructure and provides routine infrastructure operations such as patch, backup, and security management. In addition, IT management processes, such as incident, change, and service request management, are also provided. Information Builders Cloud Managed Services offers the following:

1. **Cloud Infrastructure Logging, Monitoring, and Incident Management.** Information Builders Cloud Managed Services configures your managed environment for logging activity. Working in
conjunction with the customer, Information Builders Cloud Managed Services will define additional rules regarding CPU usage and other thresholds, monitor and investigate resulting alerts that are created whenever one or more conditions from applicable cloud infrastructure-related services are triggered. When a high-severity alert is triggered, AWS Managed Services (AMS) will create a support case with Information Builders Cloud Managed Services, who then reviews and determines the next steps to diagnose and resolve the condition. In the event that the condition is related to the customer’s application or user behavior, the customer will ensure that appropriate resources are available to assist with the incident diagnosis and resolution. Information Builders Cloud Managed Services responds to incidents and resolves incidents based on the incident priority. Incidents that are determined by Information Builders Cloud Managed Services to be a risk to the security of the customer’s cloud infrastructure and Information Builders Cloud Managed Services will be proactively actioned. Premium Support Service Level Agreements (SLAs) for response time apply.

2. **Continuity Management.** Information Builders Cloud Managed Services provides backups of the AWS and Information Builders software stack using standard, existing Amazon Elastic Block Store (EBS) and Relational Database Services (if applicable) snapshot functionality on a scheduled interval determined by Information Builders and the customer. Restore actions from specific snapshots can be performed by AMS as per a Request for Change (RFC) issued by Information Builders Cloud Managed Services.

3. **Security and Access Management.** Information Builders Cloud Managed Services provides security management services, such as configuring anti-malware protection, intrusion detection, and intrusion prevention systems. Information Builders Cloud Managed Services also configures default AWS security capabilities that will be approved by the customer during onboarding, such as Identity and Access Management (IAM) roles and EC2 security groups. Customers will manage their users through an approved directory service provided by the customer.

4. **Patch Management.** Information Builders Cloud Managed Services applies and installs updates to EC2 instances for supported operating systems and infrastructure software pre-installed with supported operating systems. Customers choose a monthly one-hour maintenance window for Information Builders Cloud Managed Services to perform maintenance activities including patching activities. Information Builders Cloud Managed Services will apply critical security updates outside of the selected maintenance window. Information Builders Cloud Managed Services will apply important updates during the selected maintenance window. Patch Management is limited to the AWS stacks in the managed environment, including Information Builders Cloud Managed Services-supported AWS services with patching capabilities. Information Builders software will be patched and upgraded in coordination and consultation with the customer and Information Builders Professional Services. This patching and upgrade support does not include regression testing nor remediation of application code.

5. **Provisioning Management.** Information Builders Cloud Managed Services will provide EC2 instances for customers that are built from Amazon Machine Images (AMIs), which include the AWS infrastructure stack and Information Builders software.

6. **Support Case Management.** Information Builders Cloud Managed Services will investigate problems, attempt to identify the root cause, and remediate them either with a workaround, or a permanent solution that prevents recurrence of similar future Incidents. Customers can report issues using the [Information Builders Technical Support Center](#).
Understanding the Information Builders Cloud Architecture

This section provides an overview of the Information Builders cloud architecture, which is designed and implemented by Information Builders Cloud Managed Services. It includes the following topics:

- Provisioning Options
- Network Requirements and Considerations
- Strategy for AWS Accounts
- Customer Use Case Sample Architecture

Provisioning Options

This section describes the provisioning options that are currently available and supported by Information Builders Cloud Managed Services.

Provisioning Option 1: Pure Cloud

- Data is located in the cloud and WebFOCUS operates in the cloud.
- All IT operations and costs are offloaded to the cloud.
- Works best for new projects.
- Development can occur 100% in the cloud or from client development tools such as App Studio and Omni Designer.
Provisioning Option 2: Hybrid Cloud

- Data is located on-premises and WebFOCUS operates in the cloud.
- Data is accessed in place using a secure VPN connection.
- Existing database design and security are preserved.
- Since the data is not being staged on the cloud and is on-premises, no ETL process is required to be designed.
Provisioning Option 3: Federated Hybrid Cloud

- WebFOCUS operates in the cloud and on-premises.
- Processing of complex data operations is managed by the WebFOCUS Reporting Server on-premises.
- Network traffic between the cloud and on-premises systems is optimized.

Network Requirements and Considerations
Since cloud-based infrastructures require a customer’s focus to shift from traditional networks to WAN (Internet) connections, network admin teams must plan and prepare the network accordingly to maximize the benefits of cloud computing. This section outlines several key considerations related to Information Builders cloud network requirements. Information Builders Cloud Managed Services works in collaboration with the customer to configure the optimal network topology for the cloud instance, which includes port and proxy service configurations.

Information Builders cloud instances support 500 GB of outbound bandwidth. Web application firewalls (WAFs) are implemented to prevent a range of malicious network attacks (for example, SQL injection, cross-site scripting, and file inclusion). For more information on the designated roles and responsibilities for networking operations, see Operations: Networking.
Strategy for AWS Accounts
A number of AWS accounts (landing zones) have been established by Information Builders Cloud Managed Services in North America, Europe, and Asia Pacific to service production, internal support, and trial requirements for customers.

The following diagram illustrates our AWS account strategy, where active (live) AWS landing zones are shown.

Note: With the exception of Asia Pacific (NE - Tokyo) and (SE - Singapore), which are AWS-ready (on-demand), all other AWS landing zones shown are currently active (live).

Production customers are provisioned in country to ensure compliance with data regulatory standards. For more information, visit the following AWS Compliance websites:

- [https://aws.amazon.com/compliance/](https://aws.amazon.com/compliance/)
- [https://aws.amazon.com/compliance/programs/](https://aws.amazon.com/compliance/programs/)

Customer Use Case Sample Architecture
For reference, the following diagram illustrates a cloud environment that has been implemented by Information Builders Cloud Support for a customer use case.
Key Points:

- Each Amazon Elastic Compute Cloud (EC2) instance is provisioned with isolation from the network subnet level through AWS Managed Services (AMS) and configured security groups.

- An Elastic Load Balancer (ELB) is included, which provides full High Availability (HA) across two availability zones with the smallest exposure to the Internet required for clients to reach the applications. SSL is being used to encrypt access from the web to the EC2 instances.
• Users can be authenticated through Active Directory (on-premises or cloud) or other approach (for example, SAML).

• Access to on-premises data sources is achieved through site-to-site VPN or Direct Connect.

• Access to other cloud hosted environments (as required) is managed through VPC peering connections.

• Amazon Relational Database Service (RDS) for Oracle is deployed for failover across two Availability Zones (AZ), one per subnet.

**Information Builders Cloud Security**

Cloud security is the highest priority for Information Builders Cloud Managed Services. Customers benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

Information Builders Cloud Managed Services provides security management services, such as configuring anti-malware protection, intrusion detection, and intrusion prevention systems. Information Builders Cloud Managed Services also configures default AWS security capabilities that will be approved by the customer during onboarding, such as Identity and Access Management (IAM) roles and Elastic Compute Cloud (EC2) security groups. Customers will manage their users through an approved directory service provided by the customer.

Information Builders Cloud Managed Services assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility—particularly as it relates to customers’ data sources (e.g., on-premises data sources)—also provides the flexibility and customer control that permits the deployment. This differentiation of responsibility is referred to as Security “of” the Cloud versus Security “in” the Cloud.

**Single Sign On and Identity Management**

Information Builders Cloud Managed Services can implement single sign-on (SSO) with any identity provider (IdP), provided that Security Assertion Markup Language (SAML) support exists (service provider (SP)-initiated SAML and IdP-initiated SAML). In addition, Information Builders Cloud Managed Services can integrate with SAML-based federated authentication processes that a customer has developed and implemented in their environment.

• **Single Sign On (SSO)**

  WebFOCUS can be integrated with other Web Access Management Systems (for example SiteMinder, Oracle Access Manager, and IBM Tivoli Access Manager WebSEAL) to provide customers with a single sign-on (SSO) experience. For example, users may sign in to an existing web application with credentials that are validated by the system. If users click buttons or links that take them to a WebFOCUS portal, you may want them to be signed in to WebFOCUS automatically, rather than requiring them to provide their passwords again.
• Security Assertion Markup Language (SAML) Authentication

Security Assertion Markup Language (SAML) authentication relies on the use of a third-party identity provider to assert the authentication of a customer requesting services from a service provider. When a principal, such as a WebFOCUS user, requests services from a service provider, such as WebFOCUS, the service provider relays the request to the identity provider, who then authenticates the principal and allows the requests. SAML pre-authentication allows administrators to transfer the burden of user account maintenance to an independent provider dedicated to this task, and frees users from having to sign in multiple times during a work session, in order to open WebFOCUS and other applications. WebFOCUS supports a variety of identity providers with varying requirements for internal security and credential-based authentication. You can obtain additional information about any specialized support requirements for them by contacting Customer Support.

Information Builders Cloud Managed Services Responsibility “Security in the Cloud”

Information Builders Cloud Managed Services determines the specific AWS Cloud services to select based on a customer’s requirements. This determines the amount of configuration work Information Builders Cloud Managed Services must perform. For example, services such as Amazon Elastic Compute Cloud (EC2), Amazon Virtual Private Cloud (VPC), and Amazon S3 are categorized as Infrastructure as a Service (IaaS) and, as such, require Information Builders Cloud Managed Services to perform all of the necessary security configuration and management tasks. If an Amazon EC2 instance is deployed, Information Builders Cloud Managed Services is responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.
AWS Responsibility “Security of the Cloud”

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Note: Database and networking services as identified in this diagram can be a shared responsibility between Information Builders Cloud Managed Services and the customer.

Data Privacy: GDPR and CCPA Compliance

As an Advanced Technology Partner in the AWS Partner Network (APN), Information Builders Cloud Managed Services leverages existing compliance all AWS services have with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). As a result, Information Builders Cloud Managed Services can enable customers to achieve GDPR compliance natively on AWS, including specific measures such as:

- Encryption of personal data.
- Ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.
- Data breach notification.

For more information on AWS support with GDPR and related resources, visit the [AWS GDPR Center](#) or the [AWS CCPA Center](#).

Information Builders Cloud Onboarding Process

The following diagram illustrates the primary phases in the Information Builders Cloud onboarding process.
What to Expect on Your Information Builders Cloud Journey

Phase 1:
Cloud Architecture Planning and Design
Information Builders Cloud Support | Technical Account Manager | Customer

3 Days

Phase 2:
Provisioning of the Baseline Information Builders Cloud Environment
Information Builders Cloud Support

2 Days

Phase 3:
Establish Database Connections
Information Builders Cloud Support | Technical Account Manager | Customer

1 Week

Phase 4:
Testing Information Builders Cloud Provisioned Environment
Information Builders Cloud Support | Technical Account Manager | Customer

1 Week

Phase 5:
Formal Customer Acceptance of Information Builders Cloud Provisioned Environment
Information Builders Cloud Support | Technical Account Manager | Customer

1 Week

Phase 6:
Production Customer Support
Information Builders CSS | Premium Support

1 Week

Phase 7:
Quick Start (Self-Study) Education
Customer

26 - 30 Hours

Phase 8:
Development and Deployment: Time to Value
Customer | Information Builders Professional Services

As Per SOW

Phase 9:
User Adoption
Customer | Technical Account Manager | Information Builders Professional Services

30/60/90-Day Checkpoints
Notes and Considerations:

- **Phase 2, Provisioning of the Baseline Information Builders Cloud Environment** occurs two business days following the acceptance of the subscription contract.

- **Phase 7, Quick Start (Self-Study) Education** consists of the following self-study courses:
  
  o Course 347: Charting Techniques in WebFOCUS Designer  
    (Average Completion Time: 8 Hours)
  
  o Course 397: Putting It All Together! – WebFOCUS Portals, Pages, and Content  
    (Average Completion Time: 6 Hours)
  
  o Course 510: Metadata Essentials Using App Studio Part 1  
    (Average Completion Time: 6 Hours)
  
  o Course 511: Metadata Essentials Using App Studio Part 2  
    (Average Completion Time: 6 Hours)

Notes:

- Each self-study course provides a virtual environment that is available for 10 hours over 14 days, and in-session course materials. You will work through hands-on exercises and complete a challenge exercise to test your understanding.

- Omni-Gen education is currently being offered as instructor-led training (for example, Course 800: Master Data Management with Omni-Gen). For more information, visit the Information Builders Customer Education website.

- **Phase 8, Development and Deployment: Time to Value** is tied to the original Statement of Work (SOW). Any changes to the project scope will be managed and performed by Information Builders Professional Services, in collaboration with the customer and stakeholders.

- **Phase 9, User Adoption** occurs over a period of 30, 60, and 90 day checkpoints where ongoing usage of the Information Builders cloud provisioned environment will be closely monitored during these intervals. This will help promote user adoption by determining which enhancements or expansions may be required. Information Builders corporate account teams (including Professional Services) will collaborate and act on feedback received, to ensure cloud services continue to meet customer requirements.

**Provisioning New Information Builders Cloud Customers**

This section provides an outline of the process Information Builders Cloud Managed Services has established for provisioning new cloud customers.
Acronym Reference

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATS</td>
<td>Advanced Technical Support (Information Builders)</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>AMS</td>
<td>AWS Managed Services</td>
</tr>
<tr>
<td>CNAME</td>
<td>Canonical Name record</td>
</tr>
<tr>
<td>CSS</td>
<td>Customer Support Services (Information Builders)</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>RDS</td>
<td>Relational Database Service (Amazon)</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TAM</td>
<td>Technical Account Manager (Information Builders)</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WCS</td>
<td>Worldwide Customer Services (Information Builders)</td>
</tr>
</tbody>
</table>

1. Information Builders Cloud rider is signed and submitted to Information Builders Cloud Support (ATS).

   Corresponding phase in Information Builders Cloud onboarding process: **Phase 2**

2. TAM/account team creates an architecture diagram for the proposed environment(s) and provides the diagram to ATS.

   Corresponding phase in Information Builders Cloud onboarding process: **Phase 1**

3. TAM/account team sends the [VPN information collection form](#) to the customer or the [VPC peering information collection form](#) (if required). VPC peering is required to connect from the Information Builders Cloud AWS accounts to any resources based on the customer’s AWS accounts.

   Corresponding phase in Information Builders Cloud onboarding process: **Phase 3**

4. TAM/account team asks the customer to provide a custom FQDN for the environment. Once the environment is provisioned, ATS will request an SSL certificate from AWS for this FQDN. The custom FQDN should be within the customer’s domain. As a best practice, it is recommended to use something simple that can identify the purpose of the environment at a glance. For example:

   - reports.<customer_domain>.com
   - devreports.<customer_domain>.com

   Corresponding phase in Information Builders Cloud onboarding process: **Phase 2**

5. ATS/AMS provisions the environment based on the architecture diagram, information contained in the Information Builders Cloud rider, and the requirements of the Information Builders Cloud
software stack (WebFOCUS, Omni). Note that Omni environments may need to include provisioning of RDS databases along with standard AWS instances and network components.

**Corresponding phase in Information Builders Cloud onboarding process: Phase 2**

6. ATS/AMS creates the VPN connection on the AWS side, and provides the customer with a configuration file for the networking device specified in the [VPN information collection form](#). The customer’s network administrators create the VPN connection on their side based on the provided configuration file. If there are any issues with the customer’s configuration, ATS/AMS work with the customer network administrator to troubleshoot and test, until the VPN connection is established as required.

**Corresponding phase in Information Builders Cloud onboarding process: Phase 3**

7. ATS requests a SSL certificate from AWS for the FQDN provided by the customer. This certificate must be validated by creating a specific CNAME record inside the customer’s DNS configuration. ATS will provide the validation information. Once the validation is complete, ATS/AMS installs the certificate on the customer’s AWS environment load balancers. With the certificate installed, the customer’s DNS administrator creates a CNAME record that translates the load balancer URL to the FQDN on the certificate.

**Corresponding phase in Information Builders Cloud onboarding process: Phase 2**

8. ATS, TAM, and customer test and validate the environment.

**Corresponding phase in Information Builders Cloud onboarding process: Phase 4**

9. ATS creates a sign-off document, which certifies the initial onboarding as complete. The sign-off document will include an architecture diagram of the environment, or a build book for the environment components. The document is signed by a member from the Information Builders account team and countersigned by the customer. Note the completion of this step triggers the customer account hand-off from ATS to WCS/CSS. ATS will continue to provide assistance with any additional configuration as needed (for example, custom security implementation).

**Corresponding phase in Information Builders Cloud onboarding process: Phase 5**

10. After all Information Builders Cloud configuration is complete, WebFOCUS product support and maintenance is handled by the TAM/account team and WCS/CSS. ATS helps facilitate access to the environment and handles support for the cloud infrastructure, such as OS and networking.

**Corresponding phase in Information Builders Cloud onboarding process: Phase 6**
Roles and Responsibilities

Information Builders Cloud Support manages your AWS infrastructure. The tables in this section provide an overview of the responsibilities for activities in the lifecycle of an application running within the AWS environment.

Click your area of interest from the following list to navigate directly to the corresponding table:

- Application Lifecycle Responsibilities
- Operations: Networking
- Operations: AWS RDS Management
- Operations: Provisioning
- Operations: Logging, Monitoring, and Event Management
- Operations: Incident Management
- Operations: Problem Management
- Operations: Security Management
- Operations: Patch Management
- Operations: Continuity Management
- Operations: Service Request Management

As a guide, the following is a definition of each party that you will find listed in each table:

- **Responsible** is the party that does the work to achieve the task.

- **Consulted** is a party whose opinions are sought, typically as subject matter experts, and with whom there is bilateral communication.

- **Informed** is a party that is informed of progress, often only on completion of the task or deliverable.

Notes:

- In order to fulfill its obligations in a timely manner, Information Builders Cloud Support may require inputs from you for deciding an appropriate course of action. Information Builders Cloud Support will contact the designated customer contact for all such clarifications and inputs. Information Builders Cloud Support will expect a response to such queries within 24 business hours. In case there is no reply within 24 business hours, Information Builders Cloud Support may choose an action on your behalf.

- Some roles and responsibilities may vary, depending on how much support a customer is requesting from Information Builders Professional Services. For example, some customers are more self-sufficient than others in terms of application development within the Information Builders Cloud software stack (WebFOCUS, Omni).
### Application Lifecycle Responsibilities

<table>
<thead>
<tr>
<th>Application Lifecycle</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application development</td>
<td>Consulted</td>
<td>Informed</td>
<td>Responsible</td>
</tr>
<tr>
<td>Infrastructure requirements analysis and design</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Application deployment</td>
<td>Consulted</td>
<td>Informed</td>
<td>Responsible</td>
</tr>
<tr>
<td>Infrastructure deployment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Application monitoring</td>
<td>Responsible</td>
<td>Informed</td>
<td>Responsible</td>
</tr>
<tr>
<td>Application testing/optimization</td>
<td>Responsible</td>
<td>Informed</td>
<td>Responsible</td>
</tr>
<tr>
<td>AWS infrastructure testing/optimization</td>
<td>Informed</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>AWS infrastructure monitoring</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Troubleshoot and resolve application issues</td>
<td>Consulted</td>
<td>Informed</td>
<td>Responsible</td>
</tr>
<tr>
<td>Troubleshoot and resolve operating system, AWS network, and infrastructure issues</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
</tbody>
</table>

### Operations: Networking

<table>
<thead>
<tr>
<th>Networking</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed environment configuration</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Allocate network space for customer environment within suitable AWS account</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Configure and operate non-AMS, customer-managed firewalls/proxy/Bastions/HOSTs</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Informed</td>
</tr>
<tr>
<td>Configure and operate AWS firewalls/proxy/Bastions/HOSTs inside the managed environment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Networking configuration and implementation within customer network</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Consulted</td>
</tr>
<tr>
<td>Networking configuration and implementation within the managed environment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
</tbody>
</table>

### Operations: AWS RDS Management

<table>
<thead>
<tr>
<th>AWS RDS Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor master/slave/RO replication health</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Identify Root Cause Analysis (RCA) of</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Master Failover</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Automated snapshot (backup) configuration</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>DB engine patch management and scheduling</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Recommend instance sizing for running databases</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>RDS performance monitoring (CloudWatch)</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>RDS security group configuration</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>RDS engine parameter configuration</td>
<td>Responsible</td>
<td>Informed</td>
<td>Informed</td>
</tr>
<tr>
<td>DB table design</td>
<td>Responsible</td>
<td>Informed</td>
<td>Informed</td>
</tr>
<tr>
<td>DB indexing</td>
<td>Responsible</td>
<td>Informed</td>
<td>Informed</td>
</tr>
<tr>
<td>DB log analysis</td>
<td>Responsible</td>
<td>Informed</td>
<td>Informed</td>
</tr>
</tbody>
</table>

**Operations: Provisioning**

<table>
<thead>
<tr>
<th>Provisioning</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define managed environment architecture</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Launch managed stacks and associated AWS resources</td>
<td>Informed</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Install/Update Information Builders software stack on instances</td>
<td>Informed</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Providing third-party software licenses if applicable (for example, BYOL RDS implementations, certain DBMS clients, etc.)</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Consulted</td>
</tr>
<tr>
<td>Whitelist users for environment access via public load balancers</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Configure a VPN connection to the customer on-premises environment</td>
<td>Responsible</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Implement SSL certificates as needed for each environment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
</tbody>
</table>

**Operations: Logging, Monitoring, and Event Management**

<table>
<thead>
<tr>
<th>Logging, Monitoring, and Event Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define customer specific monitoring and incident requirements</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Configuring AWS alarms for managed environment</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Monitoring all AWS alarms</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Investigating infrastructure events for incident notification</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Investigating application alarms</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
</tbody>
</table>
Providing environment monitoring metrics to the customer | Consulted | Responsible | Informed

### Operations: Incident Management

<table>
<thead>
<tr>
<th>Incident Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactively notify Incidents on AWS infrastructure based on event monitoring</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Handle application performance issues and outages</td>
<td>Informed</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Categorize incident priority</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Provide incident response within SLA</td>
<td>Informed</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Provide incident resolution / infrastructure restore within SLA</td>
<td>Informed</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
</tbody>
</table>

### Operations: Problem Management

<table>
<thead>
<tr>
<th>Problem Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify problems in managed environment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Perform Root Cause Analysis (RCA) for problems in managed environment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Remediation of problems in managed environment</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Identify and remediate application problems</td>
<td>Consulted</td>
<td>Consulted</td>
<td>Responsible</td>
</tr>
</tbody>
</table>

### Operations: Security Management

<table>
<thead>
<tr>
<th>Security Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer infrastructure security and/or establishing baseline for security compliance process as determined and agreed to during customer onboarding</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Security group, NACL, firewall configuration</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Security infrastructure Incident handling</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Create and maintain relationship to customer managed AD</td>
<td>Responsible</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Operate federated authentication for customer access to the Information</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Consulted</td>
</tr>
<tr>
<td>Builders Cloud environment</td>
<td>Responsible</td>
<td>Informed</td>
<td>Consulted</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Add/Remove users from federated authentication system used for access to Information Builders Cloud environment</td>
<td>Responsible</td>
<td>Informed</td>
<td>Consulted</td>
</tr>
<tr>
<td>Design and Implement WebFOCUS Security Model</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Responsible</td>
</tr>
</tbody>
</table>

**Operations: Patch Management**

<table>
<thead>
<tr>
<th>Patch Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor for applicable OS updates/patches for EC2 instances</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Notify customer of upcoming patches/updates</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Exclude certain patches/updates and/or certain stacks from patching activities</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Apply OS updates/patches to EC2 instances</td>
<td>Informed</td>
<td>Responsible</td>
<td>Informed</td>
</tr>
<tr>
<td>Patch, and monitor custom and 3rd party applications</td>
<td>Responsible</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
<tr>
<td>Upgrade or patch WebFOCUS/iWay Software</td>
<td>Consulted</td>
<td>Consulted</td>
<td>Responsible</td>
</tr>
</tbody>
</table>

**Operations: Continuity Management**

<table>
<thead>
<tr>
<th>Continuity Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify backup schedules</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Execute backups per schedule</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Request backup restoration activities</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Consulted</td>
</tr>
<tr>
<td>Execute backup restoration activities</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Restore affected Stacks and VPCs</td>
<td>Consulted</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
<tr>
<td>Restore affected custom/third-party application</td>
<td>Responsible</td>
<td>Responsible</td>
<td>Responsible</td>
</tr>
</tbody>
</table>

**Operations: Service Request Management**

<table>
<thead>
<tr>
<th>Service Request Management</th>
<th>Customer</th>
<th>Information Builders Cloud Support</th>
<th>Information Builders Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request information and report issues regarding Information Builders Cloud environments using Information Builders Tech Support case management portals</td>
<td>Responsible</td>
<td>Consulted</td>
<td>Responsible</td>
</tr>
<tr>
<td>Reply to cloud-related cases</td>
<td>Informed</td>
<td>Responsible</td>
<td>Consulted</td>
</tr>
</tbody>
</table>
Information Builders Cloud Support Process

This section provides a high-level overview of the Information Builders Cloud support process and case lifecycle.

1. **Customer opens a support case through InfoResponse Live (IRL)**
2. **Information Builders Cloud customer is tagged**
3. **Application and product issues are handled by Customer Support Services (CSS)**
4. **CSS engages Information Builders Cloud Managed Services team for all cloud-related issues**
5. **CSS confirms resolution of the reported issue with customer**
Appendix A, Foundational Terminology

This section provides a reference for concepts and terms that are specific to Information Builders Cloud and also applicable to Information Builders Cloud Managed Services.

Amazon Elastic Compute Cloud Instance
An Amazon Elastic Compute Cloud (EC2) instance is a scalable virtual server that is configured to run applications on the Amazon Web Services (AWS) infrastructure. There are many EC2 instance types available based on application requirements (for example, CPU and memory demands). General purpose EC2 instances are used for WebFOCUS Total Access Cloud and Omni-Gen bundles.

For more information, visit the Amazon EC2 website.

Amazon Relational Database Service
Supported by Information Builders Cloud Managed Services, Amazon Relational Database Service (RDS) is a managed relational database service that provides you six familiar database engines to choose from, including Amazon Aurora®, MySQL®, MariaDB®, Oracle®, Microsoft SQL Server®, and PostgreSQL®. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS handles routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair.

For more information, visit the Amazon RDS website.

Application Load Balancers
Application Load Balancers (ALBs) make routing decisions at the application layer (HTTP/HTTPS), support path-based routing, and can route requests to one or more ports on each container instance in a cluster. Information Builders Cloud utilizes the latest iteration of AWS load balancing services. The following features are available:

- Whitelisting known IP addresses for secure access.
- High Availability configuration across two Availability Zones.
- Automatic redirect from HTTP to HTTPS.
- Support for custom certificates (free) and SSL configurations.
- Extended timeouts, sticky sessions, and more.

For more information, see Load Balancer Types on the AWS website.

Availability Zones
In AWS there is a concept of Availability Zones (AZs) that exist within a single region. These are clusters of data centers connected by dark fiber that are tens of miles apart. These data centers are supported by different infrastructure, power, networking, and generators. An application that has instances in two AZs has the benefit of being physically separated, while having microsecond latency as though they were located in the same physical location.

For more information, see Regions and Availability Zones on the AWS website.
Disaster Recovery
Addressed during Phase 1, Assessment of Sizing, Data Considerations, and Architecture Recommendations of the Information Builders Cloud onboarding process, disaster recovery considerations are based on the following factors that are determined by the customer’s requirements:

- **Recovery Time Objective (RTO).** The amount of time a customer is willing to accept for the product system to become available. The default is within four hours of identifying an outage.

- **Recovery Point Objective (RPO).** The amount of data loss, even if temporary, a customer is willing to accept in the event of a disaster. The default is 24 hours, based on daily snapshots.

The following disaster recovery options are currently available:

- **Pilot Light.** Database and application files are backed up. Between 10 and 20 percent of the production environment is replicated (costs would reflect this). Additional capacity can be accessed as required.

- **Warm Standby.** With this option, a subset of production instances are up and running and are 100 percent current in terms of application files and data. In the event of a disaster, the system is restored within minutes. In terms of pricing, the assumption is that 50 to 75 percent of the production cores would be required.

- **Hot Standby.** With this option, the full production environment is replicated and is always up and running. Therefore, in the event of a disaster, the disaster recovery system is available with zero downtime. Pricing is identical to that of production cores.

High Availability
High Availability (HA) architectures ensure that if a single component of an application environment fails, the application will continue to run with little to no interruption. In order for HA architectures to work, the application must support internal replication or the use of databases to maintain state and data between clustered nodes. Currently, Information Builders Cloud supports high availability in the WebFOCUS product through the following services:

- Multi-AZ load balancers
- Duplicated WebFOCUS instances in two AZs
- Multi-AZ RDS databases

Regions
In AWS, regions are clusters of Availability Zones (AZs) that are intentionally further apart from one another to provide geographic access to cloud services. This can be used to meet the requirements of disaster recovery or to place cloud services closer to your customers. For example, Information Builders is running cloud services in Northern Virginia in the AWS region called us-east-1. For more information, see Strategy for AWS Accounts in this document and AWS Regions and Endpoints on the AWS website.
Appendix B, Information Builders Cloud Site-to-Site VPN Information Collection Form

The information collected in this section helps Information Builders Cloud Managed Services create a Virtual Private Network (VPN) connection to your Information Builders Cloud environment. Ensure to include all the subnets hosting users and data, which you would like to make directly accessible to your Information Builders Cloud environment through this VPN connection.

**Prerequisites**

**Important:**

- Client remote networks/subnets must be /24 or smaller.
- Client remote networks/subnets cannot be equal to 172.26.16.0/20, since this is an AWS Cloud local management subnet.

**Notes and Considerations:**

- Your VPN will be connecting using the AWS VPN managed service. For a list of supported network devices, review the Connectivity section on the Amazon VPC FAQs Page.
- For more information about VPC configurations with your device, see the Example topics in the Amazon VPC Network Administrator Guide.
- For more information about managed VPNs in AWS, review the AWS Site-to-Site VPN User Guide.

**Customer VPN Information**

Specify the information requested in the following table, which Information Builders Cloud Managed Services requires to create a VPN configuration in AWS. Once the configuration is completed in AWS, Information Builders Cloud Managed Services will provide you with a configuration file generated specifically for the networking device type and version you specified below. In addition, Information Builders Cloud Managed Services will provide you with the AWS Primary and Redundant IP addresses.

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Primary Tunnel IP Address:</td>
<td></td>
</tr>
<tr>
<td>Redundancy Required (Yes / No):</td>
<td></td>
</tr>
<tr>
<td>Subnet details (please list all subnets you would like to access with this VPN connection):</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix C, Information Builders Cloud Site-to-Site VPC Information Collection Form

The information collected in this section helps Information Builders Cloud Managed Services create a Virtual Private Cloud (VPC) peering connection between your Information Builders Cloud environment and your own AWS account. Ensure to take note of reserved Information Builders Cloud Classless Inter-Domain Routing (CIDR) ranges mentioned below to avoid potential IP range overlaps.

**Prerequisites**

- Information Builders Cloud (Provisioning Account Name) AWS account information:
  - Account ID: *(Provisioning Account ID)*
  - VPC ID: *(Provisioning Account VPC ID)*
  - IPv4 CIDR: *(Provisioning Account CIDR)*
  
  **Note:** Peered VPCs cannot have overlapping CIDR ranges.

  - Region: *(Provisioning Account Region)*

- Customer VPCs cannot include IP address values in the 172.26.16.0/20 range, as this is a reserved Information Builders Cloud AWS management subnet.

For more information on VPC peering, see the What is VPC Peering? topic in the Amazon VPC Peering Guide.

**Customer Account and VPC Information**

Specify the information requested in the following table, which Information Builders Cloud Managed Services requires to create and initiate a VPC peering request between our AWS accounts. Once your AWS account administrators accept the peering request and the peering connection is established, Information Builders Cloud Managed Services will work with them to adjust route tables and security groups as required to establish connectivity between your Information Builders Cloud instances and your AWS resources.

<table>
<thead>
<tr>
<th>Dynamic Routing (Yes / No):</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Client BGP ASN:</td>
<td></td>
</tr>
<tr>
<td>Customer Networking Device Type and Version:</td>
<td></td>
</tr>
<tr>
<td>Required Information</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>AWS Account ID:</td>
<td></td>
</tr>
<tr>
<td>VPC ID (the VPC you would like to peer with the Information Builders Cloud account):</td>
<td></td>
</tr>
<tr>
<td>Full IPv4 CIDR used by your VPC:</td>
<td></td>
</tr>
<tr>
<td>AWS region where your VPC is hosted:</td>
<td></td>
</tr>
<tr>
<td>Subnets/IPs within your VPC to which Information Builders Cloud Managed Services will be connecting:</td>
<td></td>
</tr>
</tbody>
</table>