
BigCommerce – Service Definition (Lot 2b SaaS)

1. Service overview

BigCommerce is a fully managed Software-as-a-Service (SaaS) e-commerce platform that enables organisations to create, manage, and operate digital commerce services. It provides tools for product management, storefronts, checkout, payments, and integrations through web interfaces and APIs, without customers managing underlying infrastructure.

2. Service category and application mapping

- **Service category:** Customer relationship management
 - **Application area:** Digital commerce
-

3. Cloud deployment model

- **Deployment model:** Public cloud
 - **Multi-cloud support:** No
(Cloud infrastructure is supplier-managed and not selectable by buyers.)
-

4. Add-ons and extensions

- **Is this service an add-on or extension?** No

BigCommerce is a standalone SaaS e-commerce platform. Optional integrations and marketplace applications enhance functionality but do not constitute separate services.

5. Service features

1. Online storefront creation and management
2. Product catalogue and inventory management
3. Secure checkout and payment processing support
4. Order management and fulfilment workflows
5. Support for B2C and B2B commerce models
6. API-first architecture for headless commerce
7. Integration with third-party services and platforms
8. Role-based access controls and permissions
9. Scalable hosting and performance management

10. Fully managed cloud-based SaaS delivery

6. Service benefits

1. Enables rapid deployment of digital commerce services
 2. Reduces operational overhead for managing e-commerce infrastructure
 3. Supports scalable online sales without platform maintenance
 4. Improves customer experience through reliable checkout
 5. Enables flexible integration with existing digital ecosystems
 6. Supports growth across multiple channels and markets
 7. Simplifies management of products and orders
 8. Enhances security and reliability of online transactions
 9. Supports modern headless and composable commerce approaches
 10. Enables controlled access and governance for commerce operations
-

7. Service constraints

The service is delivered as a fully managed Software-as-a-Service solution. Buyers do not deploy or manage the underlying hosting infrastructure. Functionality is provided through configuration, supported integrations, and APIs rather than bespoke platform development. Use of the service requires internet connectivity and a supported web browser. Integration with third-party systems depends on their availability and compatibility.

8. System requirements

- Internet connectivity
 - Supported modern web browser
 - HTTPS/TLS-secured network access
 - Authenticated user credentials
 - No local installation required
-

9. Service interface

The service is accessed through a web-based management interface for administration, configuration, and monitoring of commerce operations. APIs are provided to support integration with external systems, headless storefronts, and automation of commerce workflows.

10. API access – what users can and can't do

Users can:

- Manage products, catalogues, orders, and customers via APIs
- Integrate BigCommerce with external systems and storefronts
- Retrieve commerce data for reporting and operational use
- Automate supported commerce workflows

Users can't:

- Modify or manage the underlying platform infrastructure
 - Bypass authentication, authorisation, or security controls
 - Access data outside their permitted permissions
 - Perform bespoke platform customisation outside documented APIs
 - Alter core service logic or system-level configurations
-

11. Customisation

How

Customisation is carried out through configuration using the web-based interface and supported APIs.

What

Users can configure storefronts, product structures, checkout settings, integrations, workflows, permissions, and supported commerce rules.

By whom

Customisation can be performed by authorised buyer users or approved third parties acting on the buyer's behalf. Bespoke changes to the underlying platform are not supported.

12. Onboarding and getting started

Users are supported in getting started through onboarding guidance, documentation, and access to support services. This includes assistance with initial setup, configuration, user access, and integration where required. Ongoing support is available through email and online ticketing.

13. Service metrics and monitoring

The service provides metrics relating to service usage and operational performance. These include information on storefront activity, transactions, and service availability. Metrics are available through service dashboards, reporting tools, APIs, or on request where appropriate.

14. Data protection – data in transit

Data transmitted between buyers and the service is protected using **TLS version 1.2 or above**.

15. Data protection – data at rest

Customer data is protected at rest using encryption and physical security controls in line with recognised industry standards. Access to data is restricted through role-based controls and supplier-managed security processes.

16. Data export and end-of-contract arrangements

Data export

Users can export their data using built-in export tools and supported APIs during the contract term and at contract end.

End of contract

At the end of the contract, users retain access for the purpose of exporting their data in line with agreed terms. After data extraction, access is removed and customer data is handled in accordance with data retention and sanitisation policies.

17. Support arrangements

Support is provided via email and online ticketing. Response times and support levels are provided in accordance with the agreed support terms. Technical assistance is available for configuration, integration, and service usage.

18. Availability and resilience

The service is designed for high availability using resilient, scalable cloud infrastructure. Availability is monitored continuously and incidents are managed in line with documented incident management processes.

19. Security governance

The service operates under supplier-managed security governance frameworks, including vulnerability management, incident response, access control, and protective monitoring, aligned with recognised industry best practice.