BUYING STATION

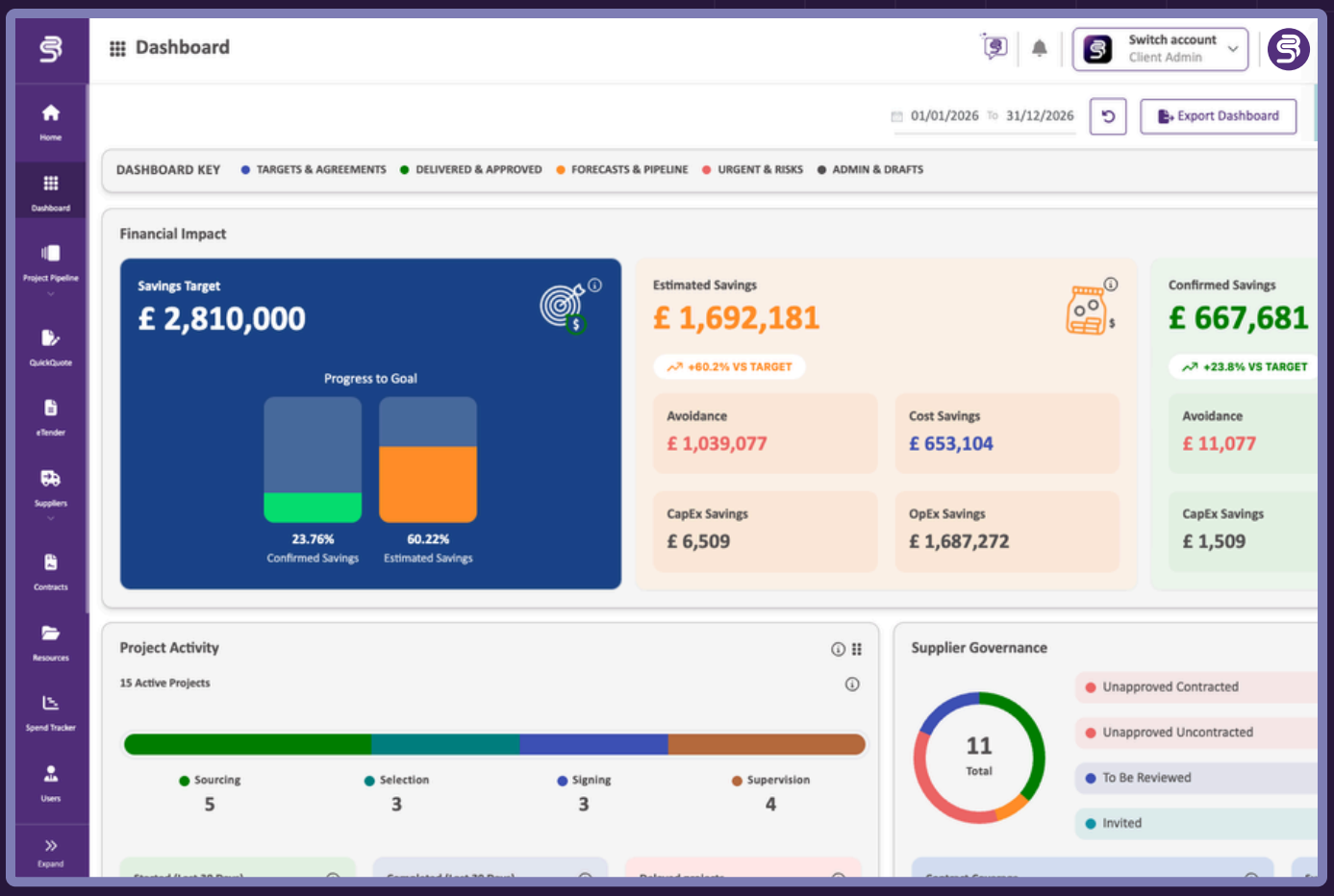
PROCUREMENT INTELLIGENCE

Technology, Security & Governance

BuyingStation

TECHNOLOGY DOCUMENT

Award Winning Procurement Intelligence
Platform for the Mid-Market



Triple ISO certified

Cyber Essentials certified

Winner, Culture of Innovation,
Amazon Accelerator Awards 2026

DOCUMENT OVERVIEW

Table of Contents

Topic	Page
About Us	03
Technology	04
Security	05
AI Consultant Security, Governance & Assurance	08
Business Continuity	10
BuyingStation Support	14
ISO Certification	15

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

COMPANY OVERVIEW

About Us

Scale confidently with BuyingStation

BuyingStation is the Procurement Intelligence Platform for the Office of the CFO, built by procurement experts who understand what it takes to scale a business and keep every commitment under control. The Source-to-Contract (S2C) platform brings supplier decisions, contract control and spend visibility into one structured view, giving your team clarity, control and confidence in every decision.

AI is being built in as an enabler, supporting your team where it adds value. New capability is rolling out through 2026. Humans keep decision authority throughout, with the people who know your business making the calls.

Whether you are a scaling business or an established mid-market organisation, BuyingStation makes sure you buy the right things, from the right suppliers, in the right way.

Purpose

Level the field; Build the future.

By bringing powerful capability within reach of teams of all sizes, we help our clients make sharper decisions, work with greater confidence and build sustainable, prosperous futures.

Vision

To be the Procurement Intelligence Platform that gives every procurement team and CFO, in every organisation, the clarity, control and insight to scale confidently.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

PLATFORM

Technology

What are the technologies used?

BuyingStation uses PSR coding language which is an open-source standardised coding style and development practise for PHP Projects. MySQL is used for database management and is managed by AWS. We use tools such as Larastan, Duster & Github Advanced security to check the code quality in conjunction with our standard quality assurance process.

BuyingStation uses separate hosting strategies for Laravel and Nuxt.js, utilising different server environments to optimise performance and scalability which consists of Laravel Hosting (Nginx Server and MySQL Database) and Nuxt.js Hosting (AWS S3 and CloudFront).

Where is our platform hosted and how is it secured?

BuyingStation is hosted on AWS which is backed up daily in the UK. AWS is a cloud computing platform offering scalable and flexible hosting solutions.

Data is transferred to AWS servers through encrypted channels (SSL) to ensure secure transmission from client devices to the platform.

AWS is considered highly secure, with a shared responsibility model:

- AWS manages the security of the cloud (hardware, software, networking and facilities).
- Customers manage security in the cloud (data, applications, identity, etc.)

AWS security features include:

- Encryption at rest and in transit.
- Identity and Access Management (IAM).
- Firewalls and DDoS protection.
- Logging and monitoring tools.

AWS complies with numerous global standards, including:

- ISO 27001, 27017, 27018 – Information security and cloud-specific controls.
- SOC 1, SOC 2, SOC 3 – System and organisation controls.
- GDPR – European data protection regulation.
- PCI DSS – Payment card industry standards
- HIPAA – U.S. healthcare data protection
- FedRAMP – U.S. government cloud security

Leading organisations including Netflix, Spotify and NASA also trust AWS for platform hosting and security.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

Where is data collection and storage held?

- **Data Collection:** Data is directly uploaded by the client through a secure user interface on the BuyingStation platform.
- **Data Storage:** All client data is securely stored in the AWS cloud servers located within the UK. Detailed Privacy policy is available at the link provided below.

PLATFORM

Security

Security Measures

1. How are updates and patches delivered and are they automatic?
Updates are deployed automatically to the web application. No action is needed from users.

2. What is the frequency of updates (scheduled or on-demand)?

- Regular updates are scheduled (e.g. every 15 days)
- Urgent fixes, like security patches, are applied instantly as needed.

3. How are customers notified of updates or maintenance windows?

- Notifications are sent via email.
- Advance notice is provided for planned maintenance or downtime.

4. Are detailed release notes provided for each update?
Yes, release notes are shared for every update, for new features, improvements and fixes.

Vulnerability Management

5. How quickly are critical vulnerabilities patched after identification?
Critical vulnerabilities are typically patched within 24–72 hours of identification, depending on complexity and testing requirements.

6. Are zero-day vulnerabilities addressed with emergency fixes?
Yes, zero-day vulnerabilities are prioritised and addressed with emergency patches to minimise risk.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

7. Does BuyingStation monitor vulnerability databases (e.g. CVE, NVD)?
Yes, BuyingStation actively monitors trusted vulnerability databases like CVE and NVD, along with other industry sources, to stay ahead of potential threats.

8. Are vulnerabilities reported by customers or third parties acted upon promptly?
Absolutely. BuyingStation has a dedicated process to validate, prioritise and address reports from customers or third parties without delay.

Security and Testing

9. What testing processes are in place before patches are released?
Patches go through rigorous testing via automation test cases and manual quality assurance reviews, to ensure reliability.

10. Are patches tested in a staging environment for compatibility?
Yes, all patches are tested in a testing and staging environment to identify and fix compatibility issues before deployment.

11. Do you conduct regular penetration tests and security scans?
Yes, we perform penetration testing, as well as perform regular security scans to identify vulnerabilities and ensure robust defences.

12. How are updates aligned with Microsoft 365 services to prevent disruptions?
BuyingStation does not currently have Microsoft 365 integrations. However, if required in the future, this will be addressed appropriately.

Customer Impact

13. Do updates or patches cause downtime and how is this communicated?
- Most updates are deployed with no downtime.
- For updates requiring downtime, customers are notified in advance via email.

14. Are rollback options available if a patch causes issues?
Yes, rollback mechanisms are in place to quickly restore the previous version if a patch causes problems.

15. Is customer action required post-update (e.g. re-authentication or validation)?
Generally, no action is required. If specific steps are needed, such as reauthentication or validations, clear instructions are provided in notifications.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

Monitoring & Reporting

16. Does BuyingStation continuously monitor for threats and vulnerabilities?
Yes, threats and vulnerabilities are monitored using advanced tools and databases.

17. Are vulnerability and patch reports available to customers?
Not at this time.

Compliance

18. Is the patching process aligned with standards like ISO 27001, SOC 2, or NIST?
BuyingStation has its own custom patching in place for managing information security and data protection. BuyingStation is proud to hold ISO 27001 certification.

19. How does BuyingStation ensure compliance with regulations like GDPR or HIPAA?
BuyingStation adheres to GDPR and HIPAA by implementing strict data protection measures, conducting regular audits and ensuring patches address compliance-related vulnerabilities promptly.

Incident and Threat Response

20. How are customers notified of vulnerabilities that impact their data or services?
Customers are promptly notified via email.

21. What is the escalation process for critical vulnerabilities (e.g. Log4j-type incidents)?
For critical vulnerabilities, the escalation process includes:

- Issue Detection: The custom logging system tracks and flags critical vulnerabilities.
- Assessment: The security team quickly assesses the severity and the potential impact.
- Fix Development: A patch or fix is developed and tested immediately.
- Deployment: The fix is deployed as quickly as possible with minimal disruption.
- Customer Communication: Customers are notified of the issue and resolution status via email.

22. Do you leverage threat intelligence to address emerging risks?
Yes, we actively leverage threat intelligence feeds and security reports to identify and address emerging risks, ensuring proactive protection against new threats.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

PLATFORM

AI Consultant Security, Governance & Assurance

BuyingStation's AI Consultant is designed with security, governance and human oversight at its core. It operates within the same controlled environment as the wider BuyingStation platform, with safeguards designed to protect customer data, respect user permissions and ensure that AI-generated insights remain grounded, explainable and auditable.

Secure Customer Data Isolation

Customer environments are securely isolated. The AI Consultant connects only to the data environment associated with the organisation making the request, preventing access to another customer's data.

This separation is enforced by the platform architecture before an AI request is processed.

Permission-Aware Access

The AI Consultant respects the same role-based access controls that govern the BuyingStation platform.

Users can only receive insights based on information they are already authorised to access. Permissions are independently enforced by the platform before data is made available to the AI Consultant, ensuring AI cannot be used to bypass existing access controls.

Controlled Data Queries

The AI Consultant does not have unrestricted access to customer databases or the ability to create arbitrary database queries.

Data requests operate through predefined and validated controls that restrict what information can be requested and how it can be retrieved. This provides an additional safeguard between the AI capability and underlying customer data.

Grounded Intelligence

AI Consultant responses are grounded in authorised BuyingStation data rather than relying solely on the AI model to generate an answer. Relevant names, dates, values and other platform information are retrieved from live data. Responses are then reviewed against the supporting data before being presented to the user.

This helps reduce the risk of unsupported or misleading information being presented as fact.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

Data Coverage & Confidence

BuyingStation provides additional assurance by assessing both the coverage of the available data and the confidence of the resulting response. Data coverage is assessed as Low, Medium or High based on the information available to support the request. A separate confidence score is then applied following review of the response.

Where supporting data is limited, confidence is deliberately constrained so that an answer is not presented as more certain than the available evidence supports. Coverage and confidence information is made visible to the user to support informed human judgement.

Protection of Sensitive Information

Sensitive fields are encrypted at rest and are only decrypted within controlled platform services when required for an authorised lookup.

Protected sensitive information is not provided to the AI model as unrestricted raw text, helping minimise unnecessary exposure of sensitive data.

Secure AI Architecture

The internal architecture of the AI Consultant is not exposed through the user interface.

Customer-facing progress information is deliberately separated from internal system details, helping protect the underlying configuration, controls and operation of the platform.

Consistent Data Processing

The underlying data retrieval layer operates consistently regardless of the user's selected interface language. This ensures that multilingual experiences do not alter the underlying data controls, retrieval process or tenant security model.

Reviewed Before Presentation

AI Consultant responses are not presented to users while the model is still generating its initial answer. Responses are held while the platform completes its review and assurance process. Only after the required checks have been completed is the response released to the user. This enables BuyingStation to prioritise answer quality and assurance while still providing a responsive, real-time user experience.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

Human-Led AI

The AI Consultant is designed to support better commercial decisions, not replace accountable decision-makers.

It can identify signals, analyse information, surface risks and opportunities, and provide directional insight. Commercial decisions, approvals and accountability remain with people.

BuyingStation combines AI capability with structured data, governance and human judgement to provide intelligence that is secure, explainable and decision-useful.

RESILIENCE & CONTINUITY

Business Continuity

Disaster Recover / Business Continuity Plan

1. Detection and initial assessment of the data breach

- BuyingStation identifies a potential data breach through monitoring, system alerts or reports from employees/third parties.
- BuyingStation to conduct an immediate initial assessment to determine the nature and extent of the breach. This includes identifying the type of data affected, the number of clients impacted and the root cause of the breach.
- The level of risk to the rights and freedoms of individuals will also be assessed. If the breach is likely to result in significant harm (e.g. identity theft, financial loss), BuyingStation will proceed to notify all relevant stakeholders.
- BuyingStation will start filling out the following Data Breach Incident Report Form.

2. Notification to the Data Protection Authority (DPA)

- Within 72 hours of becoming aware of the breach, BuyingStation will notify the relevant Data Protection Authority (DPA). This notification will include the nature of the breach (type of data and categories of people affected), the likely consequences of the breach and measures taken/proposed to mitigate the breach.
- If the notification to the DPA is beyond 72 hours, reasons for this delay will be provided by BuyingStation.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

3. Client notification of the data breach

BuyingStation will identify ALL clients whose data has been compromised as part of the breach, ensuring full accuracy in the identification process. A clear and concise data breach notification will be provided to each affected client, which includes:

- What happened: a factual description of the breach, including when it was detected and the nature of the breach (e.g. unauthorised access, data theft).
- What information was compromised: details of the categories of personal data affected (e.g. company records, financial details, contact information).
- Consequences: an explanation of the potential risks or impact on the client (e.g. identity theft, potential misuse of personal data)
- Measures taken: describes the immediate actions taken by BuyingStation to address the breach (e.g. securing systems, changing passwords, patching vulnerabilities).
- How BuyingStation are managing the situation: outlines the efforts to contain the breach and prevent any future reoccurrence, including collaborating with relevant teams to ensure security.
- Advice to the client: provides guidance on what the client should do to protect themselves (e.g. monitor all accounts, change all passwords, being alert to any suspicious activity).
- Point of contact: includes contact information for clients to ask questions, request further details or seek support (e.g. IT Support team or contact details for our DPO).

Client notification will be sent without any delay, ideally immediately after the internal assessment has been carried out and the risk has been confirmed.

4. Internal response and containment measures

- BuyingStation will implement immediate measures to contain the breach, such as revoking unauthorised access, isolating affected accounts and conducting a security audit of the platform.
- BuyingStation will establish a comprehensive plan to address the vulnerabilities that caused the breach. This includes strengthening BuyingStation's security, updating policies and improving staff training.

5. Mitigating further damage

- BuyingStation will offer support to affected clients, such as credit monitoring services, access to an IT helpline or cybersecurity advice via Apex Analytix. Ongoing updates to be provided to the client, advising them on progress.
- BuyingStation also encourages all clients to use the Multi-Factor Authentication functionality.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

6. Documentation and reporting

- BuyingStation documents the breach in high detail, including how it was detected, the steps taken to mitigate it and the communications sent to both the DPA and affected clients. This ensures compliance with the GDPR.
- A final report will be produced summarising the overall cause of the breach, how it was managed and any lessons learned. This report can be shared internally and used for audits or any further investigations.

7. Review and improvement

- BuyingStation will conduct a thorough review of the breach incident to assess the effectiveness of the response and identify any areas for improvement.
- BuyingStation will revise the company's GDPR policy, security protocols and staff training to prevent future incidents.

Data Isolation & Customer Environments

8. How is customer data separated within BuyingStation?

BuyingStation logically separates customer data so that each organisation operates within its own controlled environment. Platform controls ensure that data is associated with the correct customer organisation and is only made available within that authorised environment.

9. Can users from one organisation access another organisation's data?

No. Users can only access data associated with the organisation and environment they are authorised to use. Access controls are applied by the platform to prevent unauthorised access to another customer's data.

10. How does BuyingStation maintain data isolation when using AI?

The AI Consultant operates within the same controlled customer environment. Before information is made available to the AI Consultant, the platform validates the organisation and the user's permissions to ensure the AI cannot be used to access another customer's data.

Authentication & Multi-Factor Authentication

11. Does BuyingStation support Multi-Factor Authentication (MFA)?

Yes. BuyingStation supports Multi-Factor Authentication (MFA), providing an additional layer of account security beyond a user's password.

12. Does BuyingStation support Single Sign-On (SSO)?

Yes. BuyingStation supports Single Sign-On (SSO), allowing organisations to use their existing identity provider to manage authentication and provide users with secure access to BuyingStation.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

13. What controls are in place to protect user passwords and accounts?
BuyingStation applies security controls around user authentication and account access to reduce the risk of unauthorised access. Passwords and authentication credentials are handled securely, with additional protection available through MFA and SSO.

14. What is required from our IT department to setup SSO?
When a user clicks 'Sign in with Microsoft' for the first time, depending on the set configuration, you may need to approve the sign in on behalf of the entire organisation. Since users and licenses are managed all on BuyingStation, there is no additional setup required for an IT department.

Role-Based Access Control & Permissions

15. How is user access controlled within BuyingStation?
BuyingStation uses role-based access controls and configurable permissions to determine what functionality and information users can access within the platform.

16. Can different users have different levels of access?
Yes. Organisations can assign users different roles and permissions based on their responsibilities. This enables access to be controlled according to what an individual needs to perform their role.

17. Can access to sensitive or confidential information be restricted?
Yes. BuyingStation provides permissions and access controls that allow organisations to restrict access to appropriate users on specific modules. This supports the principle of least privilege by limiting access according to a user's responsibilities and authorised access.

18. Does the AI Consultant respect user permissions?
Yes. The AI Consultant respects the access controls applied within BuyingStation. Users can only receive AI-generated insights based on information they are already authorised to access, and the AI Consultant cannot be used to bypass existing platform permissions.

Auditability & Activity History

19. Does BuyingStation maintain a history of activity within the platform?
Yes. BuyingStation records activity and history across key areas of the platform to provide greater accountability and traceability of actions performed by users.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

20. Why does BuyingStation maintain activity history?
Activity history helps provide accountability and traceability across procurement activities. It supports organisations in understanding how information has changed, reviewing relevant user actions and maintaining appropriate governance over their procurement processes.

21. Can administrators review security-related activity against individual users?
Yes. BuyingStation provides a user history that allows users that have access to the users module to review security-related events associated with individual user accounts. This includes events such as failed login attempts and Multi-Factor Authentication (MFA) activity, including when MFA has been set up or recovered.

This provides administrators with greater visibility of account security activity and supports the investigation of unusual or potentially unauthorised access.

SUPPORT

BuyingStation Support

BuyingStation Technical Support is available between 9:00 AM-5:30 PM Weekdays GMT excluding Bank Holidays via Email and Phone. We aim to get back to you with a timeline of less than one working day.

There are many resources available on BuyingStation for support, such as fully interactive and accessible voice guided demos for all clients and suppliers

As part of Implementation for BuyingStation, there is also managed support sessions provided for users. Additional training can also be provided for suppliers and users if arranged via BuyingStation support.

Reach out to **support@buyingstation.com** for all your queries.

© Novo-K Ltd T/A BuyingStation. All rights reserved. Reg No. 10250341

British Assessment Bureau

Part of the Amtivo group

CERTIFICATE OF REGISTRATION

The management system of certificate number **265089**

Novo-K Ltd

First Floor, 17 Dukes Ride, Crowthorne, Berkshire, RG45 6LZ, United Kingdom

has been assessed and certified as meeting the requirements of:

ISO/IEC 27001:2022

BuyingStation is the trading name of Novo-K Limited and provides a ProcureTech SaaS platform offering Source-to-Contract (S2C) solutions. BuyingStation also provides Managed Procurement Services (MPS), supporting customers in delivering both strategic and tactical projects

This is in accordance with the Statement of Applicability **Version 1.1, dated November 2025.**

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

UKAS MANAGEMENT SYSTEMS

8289

Valid from:
Initial certification: 25 November 2025
Latest issue: 25 November 2025
Expiry date: 24 November 2028
Subject to annual assessments.

Authorised by

Steve Russell
Chief Governance Officer

british-assessment.co.uk

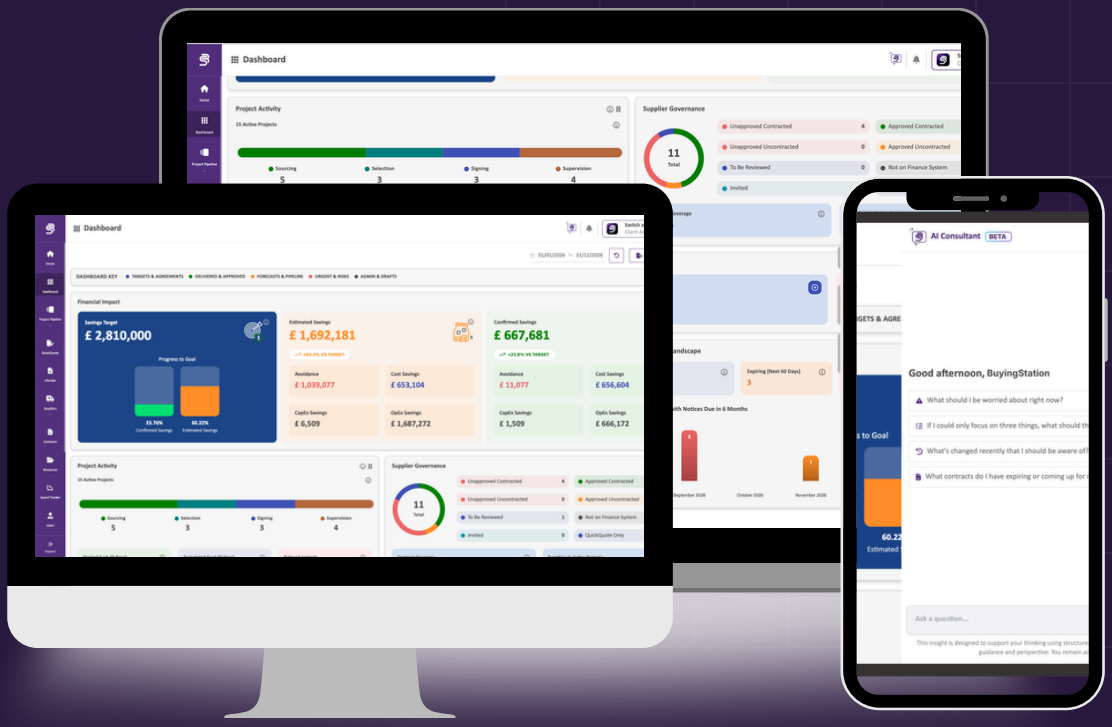
Certificate issued by Amtivo Group Limited T/A British Assessment Bureau Ltd.

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.

Amtivo Group Limited. 30 Tower View, Kings Hill, Kent, ME19 4UY.

BUYING STATION

PROCUREMENT INTELLIGENCE



Source it. Contract it. Manage it.

With BuyingStation

0330 139 7969

info@buyingstation.com

www.buyingstation.com