Business Xchange Operations and Security

Last Updated: July 2017

Contents

Compliance

- Actian maintains a SOC I Type 2 attestation on the BusinessXchange (BX) environment.
- Actian participates in the TRUSTe Privacy program.
- Actian also participates in EU-U.S. PRIVACY SHIELD FRAMEWORK.

Data Quality

How does BX ensure all transactions are successfully transmitted?

- Actian personnel monitor dashboards that show any transactions in an error state in the system, any transactions that have not reached a completed state, and any files that have some transactions unaccounted for. When data comes into BX, all transactions for that file must be accounted for and reach a completed state.

How does BX ensure data inputted is mapped correctly to the output?

- The mapping process follows customer specifications and follows a testing process that includes a User Acceptance Testing (UAT) phase where the customer approves that the data was received correctly. Any later changes to the implementation also follow an authorization, testing, and approval process. Unauthorized changes are prevented by the Change Control process.

How does BX prevent invalid data from being transmitted?

Outgoing data

- Can be validated against the syntax rules for that format (XML schema or X12 standard, for example) before being sent to the receiver.

Customer-specific

- Validation rules can be implemented—anything from required fields to making sure the line items equal the total to matching against PO data or pricebook data.

Note: Duplicate prevention is optional

Change Control

How does BX ensure mapping and configuration changes are authorized and implemented correctly?

Change authorization

- Change authorization must come from a designated account contact whose identity has been verified.

Implementation

- Mapping changes follow a testing and review process for quality control, as well as an internal approval process before changes can be made in the production environment.

Audit

- Changes to production mapping and configuration are tracked and audited for compliance.

How does BX ensure code changes are authorized and implemented correctly?

Change Authorization

- Changes to functionality or bug fixes may be requested by a user or Actian team member, but an engineering manager reviews the requested change, schedules the work, oversees the development and testing process, and approves the deployment request.

Implementation

- Changes to code follow standard procedures which include coding standards, review, and multiple levels of testing. Deployment to the production environment can only be performed by IT operations personnel following an approval process.

Audit

- Code changes and deployments are tracked and audited, with segregation of duties enforced.

How does BX ensure infrastructure changes are authorized and implemented correctly?

- Any infrastructure changes follow a multi-level approval process, and can only be performed in production by authorized IT operations personnel following an approval process.

How does BX ensure that only authorized personnel apply changes in production environment?

- BX follows policies requiring segregation of duties:
  - Engineers cannot implement changes in production
  - IT operations cannot change code
  - Approvals are tracked for all changes to production systems.

Backup and Recovery

How does BX ensure data can be recovered in case of system failure?

- A backup-and-recovery process is in place to allow rolling back to data before a system failed. Backups are also maintained at a geographically redundant data center.

How does BX ensure data can be recovered in case of human error or code error?

- A backup-and-recovery process is in place to allow rolling back to data before the data loss occurred. Backups are also maintained at a geographically redundant data center.

In case of a regional failure, will BX continue to function?

- Yes. BX data and systems are geo-replicated to a data center in a different geographical region from the primary data center to ensure business continuity for customers. The redundant system is tested to ensure the process will work if needed.

Security

Account Access

- Users can only be created when approved by the account administrator, following a secure authentication procedure to confirm the new user is authorized.

- Users can only access data for their account or the account of another division for which they are authorized.
- Users are assigned role-based functionality within BX.
- Access is restricted via a login form with controls to prevent password-guessing techniques.

Password Controls

- Initial passwords and reset passwords are randomly generated.
- Password length, complexity, reuse, and expiration have "Best Practices" standard minimums in place, and can optionally be made more stringent at the account's request.
- Passwords are stored encrypted with a non-reversible hash.
- Logins for Actian personnel are regularly reviewed, and audited access is part of the termination process when an employee leaves the company.
- Login access to the system times out after a period of inactivity.

Physical Security

- Physical security to Actian offices includes an electronic badge access system and attested to in the Actian SOC report.
- Physical security to 3rd party data centers is managed by audited 3rd party.

Data Security

Transmission

- Data can be uploaded or entered in the web portal across a secured HTTPS connection.
- Data can be sent across one of several secure channels, including but not limited to: AS2, SFTP, or RosettaNet.
- Unsecured methods such as FTP and email are supported but discouraged.
- BX supports PGP/GPG encryption/decryption.

Storage

- Customer data and transaction metadata are encrypted at rest.
- Database backups are encrypted at rest.

Proactive Threat Countermeasures

- BX stays up-to-date with security best practices, expiring less secure protocols as vulnerabilities are discovered (for example, Heartbleed and POODLE).
- BX conducts regular penetration testing to detect vulnerabilities and remediates risks that are discovered.

Availability

How does BX deliver high availability?

- BX runs in the cloud, allowing redundant services and automatic scale-out to handle high loads on demand.

How does BX handle maintenance, upgrades, and outages?

BX Maintenance

- Most updates to BX are seamless. If downtime is anticipated, the BX portal will display a notice of upcoming or current maintenance.

Customer/third-party maintenance

- Customers that anticipate maintenance or outages notify BX Support to pause delivery of transactions.
- If customers do not notify BX of an outage, the transactions will be placed on hold to be delivered later.

Disclaimer

This document is provided “as-is.” It does not constitute an agreement, contract, or warranty, expressed or implied, between Actian and any other entity. While every effort is made to keep this document up-to-date, inaccuracies or outdated information may exist within it. This document does not provide you with any legal rights to any intellectual property in any Actian product. You may copy and use this document for your internal, reference purposes.