Audit Name:	BPA #24292: IT Investments and Corporate IT: Change Mgmt. BPA #24294: IT Investments and Corporate IT: Computer Operations BPA #24296: IT Investments and Corporate IT: Logical Security
PRC 1392893	BlackLine
Process Level #1	Information Technology General Controls (ITGC)
Process Level #2	Application Development and Maintenance, Operations, and Security Processes Performed by the BlackLine Vendor
Process Owners	Mark Robertson Accounting Director/Finance Financial Control Unit Adam Bernstein Manager Accounting - Global Reconciliations, Financial Control Unit
Period Reviewed:	2019
Applicable Entities:	AIG Corporate
Updated By:	Ravi Shanker Kumar
Reviewed By:	Amit Kumar / Janet Fonseca
Reviewed Date:	4/8/19

Objective

The purpose of this narrative is to describe the Application Development and Maintenance (ADM), Operations, and Security processes and controls for the BlackLine applications that are managed by the BlackLine vendor along with complimentary processes performed by AIG.

Key Personnel Responsible for Process and Review

Adam Bernstein – Manager Accounting - Global Reconciliations

Anita Mathew – Manager, Corporate Finance IT Systems

Narrative

BlackLine is a web-based suite of applications offered through a Software-as-a-Service (SaaS) subscription model. Application Development and Management (ADM), computer operations, and certain aspects of security are managed entirely by the vendor. BlackLine holds the ISO27001:2013 certification issued by BSI.

BlackLine does not maintain its own Data Centers and instead relies upon Equinix's Ashburn Data Centers in the U.S. and Europe to host its servers. They also maintain a hot site in the Switch Data Center located in the U.S and VMware's Vcloud Air virtual data center in London, UK. Although the servers do not reside within BlackLine they are managed by BlackLine staff.

BPA #24292: Change Management and System Development Controls including Segregation of Duties (SOD)

As described in the September 30, 2018 SOC 1 ISAE 3402 report **(BL4.7),** BlackLine has a formal System Development Lifecycle (SDLC) Program to provide guidance and structure for all system development projects. The Program provides policies and standards for the Company's system development life cycle and may include the following phases:

- Project Initiation
- Analysis and Design
- Development

- Testing
- Implementation

BlackLine Senior Management determines the project type classifications and which steps of the application development or program change control process to follow. Project prioritization is based on the urgency of the request, the time required to make the change, and the objective and goals of BlackLine.

Separate environments exist for development, QA testing, sandbox, and production. Testing of all application changes includes functional system testing, regression testing and release testing. Furthermore, comprehensive penetration testing and web application vulnerability are performed on an ongoing basis by an outside security vendor. All testing results are reviewed by Information Security. If a defect is noted, the status in the project management tool is updated to reflect that additional development is required to resolve the defect. Based on the severity of the issue, the defect may be fixed and retested immediately or the change may be submitted for a future release.

Major Feature Releases

Major feature releases strictly follow the five phases of the SDLC. Major feature releases includes one or more of the following: new modules, a related set of normal changes, projects that may require multiple team members, and projects that are large in scope. All approved projects are entered in the project management tool.

The Project Initiation phase encompasses the following steps: initiate the kickoff meeting, obtain project approval, and assemble the project team. During the Analysis and Design phase, business and security data requirements documentation is created by the project team. User and system documentation, as well as coding is performed during the Development phase of the project. The Testing phase involves the QA of the defined system changes, and the Implementation phase relates to the process of releasing of the system into production.

Release to production is authorized by Management and the Change Management Board (CMB). A maintenance window is scheduled and clients are notified in advance. Clients and internal users are notified of upcoming releases via a public-facing web site (trust.BlackLineBlackLine.com). Maintenance is typically not scheduled during calendar financial close periods. Release notes are created for program changes that are appropriate for end users in order to aid clients with the release. Additionally, webinars are held by BlackLine personnel on how to use the new features when applicable.

In the event of failure of a major application feature release "Resolve Immediately" JIRA issues are documented and addressed immediately .JIRA has standard classifications to assign to each ticket," Resolve immediately" being one of them.

The source code for each major release is tagged and assigned a specific version number. BlackLine uses version control software tools, for managing and tracking development code changes. Developers have access to check in, modify and check out BlackLine application source code within the development environment. Developers cannot access the production environment. Lead Delivery Engineering personnel maintain required access to the development and production environments in order to migrate and deploy releases. To ensure appropriate segregation of duties, a required "Merge Checks" configuration is implemented for the application code repository, requiring two unique and separate authorized individuals to approve code commits to the repository. Changes to the "Merge Checks" configuration is restricted to administrators with all configuration change events logged and available for review.

Change Management Board

BlackLine has established a Change Management Board (CMB) to review all client facing changes. The CMB is comprised of Senior Management representing Corporate IT, Technology Operations, Client Support, Information Security, and Product management. CMB meets daily to discuss, review, and approve changes.

AIG Testing

Based on our discussions with Adam Bernstein, AIG has created a 'sandbox' environment where the BlackLine vendor places the new release. This allows AIG staff to familiarize themselves with the new release, adjust to any new functionality, and test file uploads in a non-production environment. Unlike the Corporate production environment, BlackLine System Administrators allow Local Administrators to upload files into the sandbox environment.

All users have the same level of access in the sandbox environment as they do in production, the only difference being that local administrators for the corporate instance of BlackLine have the ability to upload data (a privilege that is reserved for the system administrator in the production environment). In addition, the sandbox environment is generally refreshed monthly with a copy of the production environment so that all data is up-to-date.

Change Management

A Change Management Policy is in place that describes the change control process for major feature releases, application changes, and infrastructure changes. The policy is reviewed and updated as needed. BlackLine has classified application changes and infrastructure changes into four categories: normal, urgent, emergency and standard operating procedures (SOP) changes. Requests for each infrastructure/hardware chance require approval from manager of the team performing the change and all five CMB representatives. Application changes (i.e., user interface changes, new features, reporting, etc.) are initiated when a business need arises that affects the BlackLine application or software. These changes can impact major/minor releases, hotfixes and micro services. In addition, infrastructure changes are initiated by events such as the procurement of new hardware or maintenance, such as patching. Change request forms are completed for all application and infrastructure changes to document and track management's approvals within the project management tool. Additionally, BlackLine maintains an Asset Management Policy for tracking assets.

Normal Changes

Normal Changes are the most common type of change. These types of changes follow the standard change control process of being implemented into production after receiving manager and CMB approval. Requests for a normal change can be submitted by the end-user or initiated by BlackLine personnel as part of the Company's ongoing effort to provide the best product and service to its clients.. When a normal change, either application or infrastructure related, is ready to be pushed to production, a Request for Change (RFC) ticket must be created. All tickets require manager approval before being submitted to the CMB for review and approval. Normal application change requests that affect production are developed and tested. Normal infrastructure changes do not require QA testing. Once the change is approved by CMB, the change is implemented into production. Normal changes typically encompass internally-developed software projects that are smaller in scope than major changes, as well as infrastructure related changes. Examples may include feature changes and non-emergency defects. All approved projects are entered in the project management tool.

Urgent Changes

An urgent change request is defined as a request that needs to be implemented before the next scheduled CMB meeting. Before an urgent change can be implemented into production, the approval of the manager is required. Once approved, the urgent change needs the approval of at least two members of the Urgent Change Management Board (UCMB) before the change can be implemented into production. A post-implementation review is performed for all urgent changes at the next CMB meeting for the appropriateness of the urgency. Any comments or issues caused by the urgent change request are documented.

Emergency Changes

An emergency change request is defined as a request that requires immediate processing and if not implemented immediately will result in daily processing delays and/or system breakdowns. Emergency change requests are documented in JIRA after the change is implemented into production, which still require manager approval. A post-implementation review is performed for all emergency changes at the next CMB meeting to understand the root cause and measures to prevent future occurrences.

Standard Operating Procedures (SOP) Changes

A Standard Operating Procedures (SOP) change request is a standard, typically non-customer impacting change that occurs on a regular basis. SOP changes require manager and CMB approval prior to the creation of RFC-minor sub tickets. A RFC-minor sub-ticket is generated for each instance of the change being implemented by the individual performing the change. Each SOP change is reviewed on an annual basis by the CMB to determine if the SOP is still necessary.

BPA #29294: Operational Controls

Backup Monitoring

The backup process for key client data files and programs are monitored to ensure that backups are processed to successful completion. As described in the September 30, 2018 SOC 1 ISAE 3402 report, BlackLine uses Commvault to perform backups of its production servers.

The backup process is monitored by BlackLine Operations personnel. If there are any failures in the daily backups, an alert e-mail is generated to BlackLine for immediate review and follow-up. Backup logs are maintained within Commvault for review and analysis.

To ensure system and client data availability in the event of a disaster, BlackLine has established an alternate processing site in a remote location separate from the production site. To ensure a high degree of availability, data is pushed or synchronized between the hot site and the production system every hour. All data pushes are monitors via InMage dashboard for any potential problems.

Two data centers serve as backups to each other. BlackLine replicates production data from Switch’s Las Vegas to Equinix’s Ashburn data center for its U.S based production operations. BlackLine replicates production data from Verizon’s Amsterdam data center to VMware’s London virtual data center for its EU-based production operations.

Commvault encrypts as it performs backups.

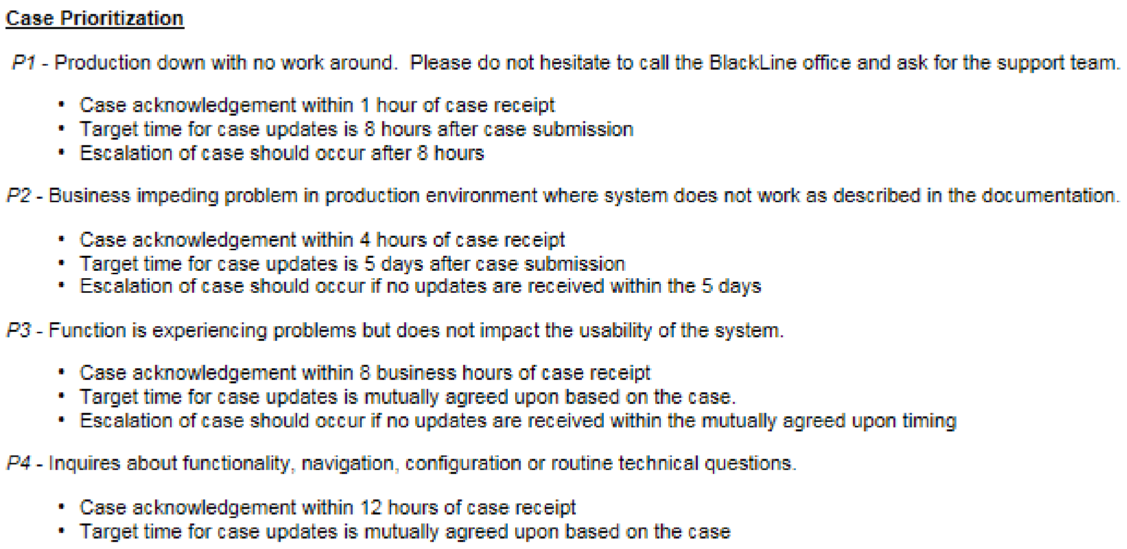
Job Monitoring

Batch processes are run on client-defined schedules to obtain data for processing by BlackLine. Once data is placed by the client on the server, it is removed for processing by the BlackLine automated scripts. BlackLine’s FTP site is configured to restrict client access to only their specific file directories and clients do not have access to other client directories or files.

Production Environment Monitoring

Microsoft System Center Operations Manager (SCOM) is installed to monitor system performance and the identification of any potential server problems. Alerts are generated by monitoring tool and sent to Technology Operations for immediate follow-up. BlackLine reviews and tracks alerts to completion.

Advanced performance and application monitoring tools have been deployed to monitor application response times from various global locations, as well as to detect and isolate problems before they impact clients. BlackLine clients are responsible for notifying BlackLine if they experience problems or issues. The problems are recorded and logged via an online BlackLine support portal as ‘cases’. It should be noted that this portal is not part of the BlackLine application suite and requires a separate login. Only the BlackLine System Administrator has the capability to log cases. Cases are assigned one to the following four designations:



Case Prioritization

P1 - Production down with no work around. Please do not hesitate to call the BlackLine office and ask for the support team.

- Case acknowledgement within 1 hour of case receipt
- Target time for case updates is 8 hours after case submission
- Escalation of case should occur after 8 hours

P2 - Business impeding problem in production environment where system does not work as described in the documentation.

- Case acknowledgement within 4 hours of case receipt
- Target time for case updates is 5 days after case submission
- Escalation of case should occur if no updates are received within the 5 days

P3 - Function is experiencing problems but does not impact the usability of the system.

- Case acknowledgement within 8 business hours of case receipt
- Target time for case updates is mutually agreed upon based on the case.
- Escalation of case should occur if no updates are received within the mutually agreed upon timing

P4 - Inquires about functionality, navigation, configuration or routine technical questions.

- Case acknowledgement within 12 hours of case receipt
- Target time for case updates is mutually agreed upon based on the case

There is a Service Level Agreement (SLA) between AIG and BlackLine that designates the maximum amount of time required to address/correct each case level. Additionally, there is a bi-weekly meeting with BlackLine Production Support to review any open cases.

BPA #29296: Logical User Access and Security Controls

Security Administration
To protect BlackLine's assets and client data, an Information Security program guided by written Information Security Policies and Standards which contain details of purpose, scope, and specific information security requirements have been established. These standards are applicable to all BlackLine employees and vendors. The policy is made available to all employees.

BlackLine Information Security Program is reviewed annually by Information Security Management.

The policy follows ISO27000 series of standards and includes specific requirements for Electronic Mail Security, Virus Protection, Logical Access, Security Monitoring, Acceptable User Policy, Password Standards, Disaster Recovery, Risk Assessments, User Provisioning, Vendor Management, and Incident Response. BlackLine holds ISO27001:2013 certification issued by BSI

Server Configuration Monitoring and Password Settings

Network and firewall security configurations and settings are reviewed on an annual basis. This is done to ensure compliance with BlackLine Security Policies and meet current security and availability requirements.

BlackLine is capable of enforcing all key password parameters for SOX. All passwords must be a minimum of eight characters long, include mixed-case letters, digits, and special characters and are set to expire every 90 days. The settings for minimum length (8 characters) and expiration (90 days) are hardcoded into the application and can only be changed by the vendor. The setting for account lockout is configurable by the AIG System Administrator and has been set to six attempts.

Data Center Access

As described in the September 30, 2018 SOC 1ISAE 3402 report, BlackLine's infrastructure and applications are located in dedicated spaces within Verizon's data centers in Amsterdam, Netherlands, Switches data center in Las Vegas, Nevada and Equinix's data center in Ashburn, Virginia. BlackLine also leverage's VMware's vCloud Air virtual data center in London, UK. Physical access to the data center is restricted 24x7x365 via identity badges, electromechanical locks, and closed circuit video. Smoke and floor water detectors, raised floors, detection suppression systems, and fire detection systems are utilized to detect and prevent environments hazards.

Data center access is limited to appropriate personnel. . Only authorized BlackLine employees are allowed to modify the physical access listing.

As a part of vendor management, BlackLine's Information Security team annually reviews all third party data center provider's SOC 2 type 2 controls.

Privileged Access Monitoring

BlackLine performs a monthly review of privileged and administrative accounts including user accounts that have access to clients' data. The review is managed by Information Security, where management of Technology Operations, Database Operations, Corporate IT, Support, Customer Success Managers, and Implementations team perform the review.

Network Security Monitoring

Information Security – External network intrusion detection software and sensors are in place to monitor potential unauthorized access to BlackLine's networks. User security violations are logged and reviewed. Tickets which are created for all incidents are reviewed and closed out by management as they are resolved.

As described in the September 30, 2018 SOC 1 ISAE 3402 report, BlackLine utilizes an Intrusion Detection System (IDS) to monitor network traffic on a real-time basis. Security alerts are logged and followed up by BlackLine-designated personnel or contractors as needed. BlackLine transitioned from utilizing ProtectWise to Snort as its IDS in July 2018. Additionally, Security Operations team utilizes Nexpose to conduct internal vulnerability scans on a weekly basis to identify any vulnerabilities within the network.

Internal access events such as logons are logged and stored in a centralized log management server. Specific types of events which are logged are defined within the security policies. Tickets are created to document the resolution of identified critical security events. Log reviews are performed as needed to identify and resolve incidents involving potential or actual unauthorized activity. BlackLine utilizes InsightIDR to perform first level monitoring of security violations and user activity..

In addition, BlackLine conducts a series of security assessment activities, including:

- Automated and manual web application security assessments
- Source code scanning
- Weekly infrastructure vulnerability assessments
- Annual penetration tests

Anti-virus and malware protection tools are provisioned on workstations and servers.

Encryption

Client Data entered via the web is protected using TLS certificates with 2048-bit keys and 256-bit encryption.

Client files and databases at rest are encrypted using 256-bit AES. The encryption is accomplished using the Vormetric and Kaminario tools. Both tools control access to encrypted information using a series of rules. Only authorized applications and individuals can access client data.
Employee workstation and laptop hard drives are encrypted and managed via endpoint encryption solutions.

Data Integration

BlackLine provides its clients the option of transmitting data securely utilizing File Transfer Protocol (FTP) servers. Clients utilizing the FTP feature are given the option of choosing the type of encryption to protect their data – Secure FTP (SFTP), FTP secure (FTPS), Pretty Good Privacy (PGP) keys, or a combination. The client indicates their desire to use SFTP/FTP servers on the Remote Access Request Form. This serves as authorization to establish an SFTP/FTP account.

The client must go through a sign-on process to gain access to the SFTP and FTP site. A unique user ID and password/public key are required before access is granted.. BlackLine's SFTP/FTP site is configured to restrict client access to only their specific file directories and clients do not have access to other client directories or files.

Changes from Prior Year

As of April 2019, Dhimant Patel, Solutions Architect, Corporate Functions, Investments & Corporate IT, is no longer with AIG. His manager, Anita Mathew, is temporarily taking over his duties.

Also, the production data center has moved from Switch's Las Vegas data center to Equinix's Ashburn data center.

Flow of Transactions

Flowchart Reference: *N/A*

Key Control Identified

Control CA-1404922 (~~IT-CM-R1-C1~~) – BlackLine has established separate environments for development, QA testing, sandbox, and production. Developers cannot access the production environment

Control CA-1404933 (~~IT-CM-R2-C2~~) – BlackLine Development tests all application changes and performs functional system testing, regression testing and release testing. Release to production is authorized by BlackLine Management and BlackLine Change Management Board.

Control CA-1404923 (~~IT-OPS-R12-C12~~) – As needed, BlackLine uses Commvault to perform backups of its production servers. The backup process is monitored by BlackLine operations personnel. If there are any failures in the daily backups, as an alert email is generated to BlackLine for immediate review and follow-up.

Control CA-1404925 (~~IT-OPS-R14-C14~~) – Alerts are generated by monitoring tools (NetApp, SolarWinds, Logic Monitor) and sent to Technology Operations for immediate follow-up. BlackLine reviews and tracks alerts through to completion. Note: This control may be removed from SOX scope.

Control CA-1404926 (~~IT-SDI-R4-C4~~) – Major feature releases strictly follow the five phases of SDLC namely; Project initiation, analysis and design, development and testing and implementation. Note: This control may be removed from SOX scope if there are no major projects planned that could impact the financial statements.

Control CA-1404929 (~~IT-SEC-R7-C7~~) – Network and firewall security configurations and settings are reviewed on an annual basis. This is done to ensure compliance with BlackLine Security Policies and meet current security and availability requirements.

Control CA-1404930 (~~IT-SEC-R8-C8~~) – Physical access to the data centers is restricted 24x7x365 via identity badges, electromechanical locks, and closed circuit video. Smoke and floor water detectors, raised floors, detection and suppression systems, and fire detection systems are utilized to detect and prevent environmental hazards. Note: This control may be removed from SOX scope.

Control CA-1404931 (~~IT-SEC-R9-C9~~) – Monthly, a review of privileged and administrative accounts is performed.

Control CA-1404927 (~~IT-SEC-R10-C10~~) – BlackLine utilizes ProtectWise to monitor external networks on a real-time basis. Security alerts are logged and followed up by BlackLine-designated personnel or contractors as needed. Note: This control may be removed from SOX scope.

Risk & Control Matrix

RCM Reference: *2019 SOX Risk and Control Matrix*

Testing Nuances

The 2019 SOC 1 ISAE 3402 report for BlackLine will be reviewed to confirm if these controls are operating effectively.

Spreadsheet Index

*********************************** **End** ***