Ex Libris Cloud Services BCP

Version 2.0

A newer version is available here

Business Continuity Plan Overview

The Ex Libris Group Cloud Services Business Continuity Plan is a comprehensive statement of actions to be taken before, during and after a disaster. This plan is designed to reduce the risk to an acceptable level by ensuring the restoration of critical functions and services within a short time frame, and all essential production within a longer, but permissible, time frame. This plan identifies the critical functions and services for Ex Libris cloud services and the resources required to support them. Guidelines and recommendations are provided for ensuring that needed personnel and resources are available for disaster preparation, assessment and response to permit the timely restoration of services.

Definitions

Business Continuity Plan (BCP) - a document describing a set of arrangements, resources, and sufficient procedures that enable an organization to respond to a disaster and resume its critical operations within pre-defined time frame without incurring unacceptable operational impacts.

Disaster Recovery Plan (DRP) – a technical document describing the processes, policies, and procedures related to implementing precautionary measures and preparing for the recovery, continuation, or resumption of services in the event a catastrophic event occurs.

Disaster – a sudden, unplanned calamitous event that causes a complete loss or significant disruption in customer's mission critical services. The primary objective of the plan is to minimize the risk of low-level events and minimize the impact of major high-level events.

Business Continuity Plan Objectives

The principal objective of the business continuity plan is to develop, test and document a well-structured and easily understood plan which will help Ex Libris cloud services recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts Ex Libris cloud services and business operations.

The objectives of this document are:

- Develop a Business Continuity Plan structure for managing a disaster that affects the Ex Libris cloud services.
- Document critical information and procedures as required for the implementation of the Business Continuity Plan.
- Present a course of action for restoring critical cloud services within a minimum number of days of initiation of the plan
- Provide guidelines with an escalation plan for a disaster declaration that will result in the execution of this Business Continuity Plan.
- Describe an organizational structure for carrying out the plan and ensure that all employees fully understand their duties in implementing such a plan.
- Ensure an orderly recovery after a disaster occurs, minimizing risk of lost production or services

Business Continuity Plan Policy

Ex Libris management has approved the following policy statement:

- The company shall develop a comprehensive Business Continuity Plan.
- A formal risk assessment shall be undertaken to determine the requirements for the Business Continuity Plan.
- The Business Continuity Plan should cover all essential and critical infrastructure elements, systems and services, in accordance with key business activities.
- The Business Continuity Plan should be periodically tested to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All Ex Libris cloud services staff must be made aware of the Business Continuity Plan and their own respective roles.
- The Business Continuity Plan is to be kept up to date to take into account changing circumstances.

Assumptions of the Plan

The Business Continuity Plan has been developed and maintained based on the following assumptions:

- This document plans for the major/worst case disaster. However, if an outage of services occurs to a lesser degree, this plan will cover the incident.
- The situation that caused the disaster is localized to one of Ex Libris data center locations (Chicago, Amsterdam or Singapore).
- Ex Libris cloud services are utilizing a co-location agreement with a leading data center facilities provider (Equinix). The facilities provider will provide the baseline infrastructure needs in the event of an emergency.

BCP Team Descriptions and Responsibilities

- **BCP Management Team** - Responsible for the overall direction, decision-making, and approvals required to implement the Business Continuity Plan. The team is comprised of the Ex Libris Chief Operating Officer (COO), and cloud services directors who are responsible for leadership within their respective areas.
- **Business Continuity Coordinator (BCC)** – A member of the BCP Management Team with responsibility for the development, coordination, training, testing and implementation of the Business Continuity Plan.
- **BCP Team Leaders** - Responsible for carrying out the tasks and provisions of the Business Continuity Plan including assigning tasks to staff, obtaining offsite data backups, contacting vendors, monitoring work progress and reporting the status to the BCP Management Team. The team is comprised of all Ex Libris cloud services team leaders and managers.
- **Emergency Operations Center (EOC)** – A location established by the BCP Management Team for central coordination during the recovery efforts. This location will typically be established at Ex Libris group headquarter offices.

Disaster Risks and Prevention

As important as having a Business Continuity Plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, and steps we should take to minimize our risk. There are many forms of catastrophic loss that can occur. This section lists some of the events and situations that are considered when determining what to include in the plan.

Preventive Measures

Potential Disaster	Preventive Measures
Equipment/hardware failure	Redundant infrastructure - This is addressed by Ex Libris in its architecture and design standards at all infrastructure layers including multiple Firewalls, Switches, Storage controllers, Load balancers, manageable PDU's, cabling, Power sources, and standby hardware. Premium grade hardware support contracts with short SLAs for onsite repair or replacement for all Cloud infrastructure hardware – The result is reduced time for replacement of failed servers, drive arrays, and network equipment. Multi Network providers redundant internet connections - This is addressed by Ex Libris in its network architecture and implementation standards in conjunction with services from the ISP to support the requirements.
System and Software Failure (data corruption, programming errors)	Data backups – At all layers, including platform, application, and customer data 24/7 application and technical support – This is addressed by the Ex Libris Group, 24/7 Hub (NOC). Use of disk protection shared storage technology at the platform and application level
Power outage	Uninterruptible power supply (UPS) and backup generators to keep systems going in the event of a power failure - data centers feature full UPS power, back-up systems and N+1 (or greater) redundancy. This service is supplied by the facilities provider. Redundant power, cooling – An effective and efficient cooling infrastructure that is robust enough for the most complex high-power density deployments. This is addressed by Ex Libris in its network architecture and implementation standards in conjunction with services from the facilities provider to support the requirements. Surge protection to minimize the effect of power surges on electronic equipment - This is addressed by the facilities provider, by implementing both facilities grade protection as well as surge protected power strips at the rack level.
Malicious Activity (security violations, denial-of-service attack, sabotage, act of terrorism)	Physical access security – 24/7 security, biometric authentication, video surveillance, authorized personnel. Infrastructure security - Hardening, change management procedures, Risk Assessment, patch management, password policy, audit and review by Ex Libris Chief Information Security Officer (CISO) Network security – Segregation, Vulnerability scans, Intrusion Prevention System (IPS), TLS/SSL encrypted communication. Application security - Security Development Lifecycle (SDL), Penetration tests, vulnerability assessment, OWASP Top10, audit and review by Ex Libris Chief Information Security Officer (CISO). Data security - Data isolation, encryption, segregation, media sanitization (DoD 5220.22-M). Identity & Access Control - SSO, S/LDAP, SAML/Shibboleth, Role-Based Access Control (RBAC). Monitoring & Incident Management - 24x7 monitoring, Chief Information Security Officer (CISO), security breach notification. Human Resources - Security awareness training, confidentiality agreements, adherence to regulations Compliance & Audit - ISO 27001, SSAE-16, EU Safe Harbor, Data processing agreements, independent audit.

Potential Disaster	Preventive Measures
Natural Disasters (earthquakes, floods, storms, tornados, hurricanes, natural fires)	Fire preventions — VESDA (Very Early Smoke Detection Apparatus) installed for early warning; analog addressable fire detectors at 3 levels installed; automatic high pressure hi-fog system alarms, CO2 fire extinguishers, and flame suppression systems are supplied by the facilities provider. 24/7 onsite facilities support – Operation personnel are 24/7 on site and together with security staff fully trained in basic firefighting (hand held extinguishers) with strict procedures in place to deal with emergencies including evacuation. This is addressed by the facilities provider, Smart Hands Services. Flooding - Flooding is reviewed with the FEMA maps (or equivalent) and 100 year flood plains during building area locations and design. This is addressed by the facilities provider, Smart Hands Services. Earthquakes - The building code takes into consideration the geographical regions, the type of soil the foundation sits on and the function of the building (data centers are occupancy group III), then assigns Seismic Design Categories (A thru F) that structural engineers base their calculations on. This is addressed by the facilities provider.

Redundancy Strategies

The following are the redundancy strategies available in the Ex Libris Group Cloud Services environment:

- **Active/Active Load balancing** - Traffic is split evenly between 2 or more servers for critical servers. Upon failure of one of the servers, traffic is shifted automatically and seamlessly to the working server.
- **Active/Active Anti-virus** – traffic is split between 2 or more anti-virus scan devices for balancing. The traffic is shifted automatically and seamlessly to the working server.
- **Active/Passive Network** – The External Network comes from a primary dedicated line with automatic failover into a secondary dedicated line. The internal network is redundant at all layers.
- **Active/Passive Multiply ISP providers** – Multi ISP connected to the primary site using Managed Internet Route Optimizer with automatic fail over.
- **Active/Passive Firewall** – Network traffic uses primary Firewall with automatic failover to a secondary Firewall.
- **Active/Active Storage** – Data is split between 2 or more storage controllers for balancing and take over in case of fail.
- **Available on-site servers' capacity** – Also referred to as "Onsite Cold Equipment". In the event a catastrophic hardware failure takes place and cannot be resolved in a timely manner, the virtualized instance of the customer's hosted environment will be mounted from an existing standby server that has been preloaded with the appropriate OS and administrative applications. In case needed, the customer's data restoration would then be performed from onsite or from offsite backups.

Backup Strategies

Ex Libris has a well-developed backup plan consisting of multiple daily snapshots including a full daily backup. The backups are made to a separate set of disks which offers a much more reliable fast retrieve backup media, and is stored at the site and in a remote secured location over a private dedicated fast secured line. This guarantees that at any point in time, in case of a disaster, Ex Libris holds copies of the data onsite and in a remote and secured disk backup. On a regular basis, Ex Libris performs a system backup to back up application files, database files, and storage files. The privacy controls in practice at the company apply as well to all backup files. All backup files are subject to the privacy controls in practice at Ex Libris. The restore procedures are tested on an ongoing basis to ensure rapid restoration in case of data loss.

- **On-site backup** – Full backup for OS platform, application, and customer data are performed at least daily (multiple snapshots during the day for critical services/systems) using storage snapshot technology. The backups are kept for one week on-site at a separated set of disks. The snapshots are automatically mounted with specific access restriction values seen by the operating system in a special set of directories allowing for an easy and immediate restore at any

time by Ex Libris authorized personnel.

- **Off-site backup** – Full backup for OS platform, application, and customer data are performed daily using snap mirror technology over a private dedicated fast secured network connection from the primary data centre to an off-site backup location using the same storage technology as the storage at the primary location. Subject to the privacy controls in practice at Ex Libris, Ex Libris maintains the off-site backup locations in the same territory (NA, EMEA, and APAC) as the primary locations with a sufficient best practice physical distance. The backups can be retrieved back to the main data centre 24/7 by Ex Libris authorized personnel. The backups are kept at the off-site backup managed locations.

Disaster Detection and Determination

The detection of an event which could result in a disaster affecting Ex Libris cloud services is the responsibility Ex Libris' 24x7 HUB or whoever first from the Ex Libris cloud group that discovers or receives information about an emergency situation developing in one of the functional areas of the cloud services.

Disaster Notification

Whoever detects the disaster should notify the Ex Libris Cloud Operations Director or the Ex Libris Cloud Engineering Director. In addition to providing some fault tolerance in the initial response, this role sharing enables effective use of shifts during the disaster recovery process.

The Ex Libris Cloud Operations Director or Ex Libris Cloud Engineering Director will establish the Emergency Operations Center (EOC) and monitor the evolving situation and, if appropriate, will then notify the BCP Management Team. The complete emergency contact list for the Ex Libris cloud services is included in Appendix A.

Normally, the facilities provider's Network Operation Center (NOC) and/or the local law enforcement receive the initial alarm notice through their monitoring system capabilities. If the emergency does not activate a normal alarm system, these two parties should immediately be notified by the Ex Libris Cloud Operations Director or Ex Libris Cloud Engineering Director.

Determine Personnel Status

One of the Ex Libris Cloud Operations Director or Ex Libris Cloud Engineering Director's important early duties is to determine the status of personnel working at the time of the disaster. Safety personnel on site after the disaster will affect any rescues or first aid necessary to people caught in the disaster. However, the director should produce a list of the able-bodied people who will be available to aid in the recovery process. Taking care of people is a very important task and should receive the highest priority immediately following the disaster. While we will have a huge technical task of restoring computer and network operations ahead of us, we can't lose sight of the human interest at stake.

Damage Assessment

To determine how the business continuity plan will be implemented following a sever disruption to service, it is essential to assess the nature and extent of the damage to the system.

Once the appropriate facilities provider's contacts have been notified, the BCP Team Leaders will be contacted so that a preliminary determination can be made whether an onsite damage assessment is required or feasible.

Damage assessment is intended to establish the extent of damage to mission critical computing devices and the facility that houses them as quickly as the given conditions permit, with personnel safety remaining the highest priority.

The following areas should be addressed:

- Cause of the disaster or disruption
- Potential for additional disruptions or damage
- Area affected by the disaster
- Status of physical infrastructure (e.g., structural integrity of data center, condition of electric power, telecommunications, and heating and ventilation/environmental conditions)
- Inventory and functional condition of Ex Libris equipment
- Type of damage to equipment or data (e.g., water, fire, physical impact, electrical surge)
- Estimated time to restore normal services

Disaster Determination

The key outcome from the Damage Assessment process is to determine the severity of the disaster and to estimate the amount of time required to restore the Ex Libris cloud services back to normal operations.

The Ex Libris cloud services group has classified disasters and emergencies into the following three levels – minor, major and catastrophic:

- **Minor Disaster** - A minor disaster will be characterized by an expected downtime of no more than 48 hours. Damage can be to hardware, software, and/or operating environment. Ex Libris cloud services could be restored to normal operations at the primary site and repairs can be started as soon as possible:
- **Major Disaster** - A major disaster will be characterized by an expected downtime of more than 48 hours but less than 7 days. A major disaster will normally have extensive damage to system hardware, software, networks, and/or operating environment. Ex Libris cloud services could be restored to normal operation with the assistance of certain recovery teams who will be called to direct restoration of normal operations at the primary site.
- **Catastrophic Disaster** - A catastrophic disaster will be characterized by expected downtime of greater than 7 days. The facility is destroyed to the extent that an alternate facility must be used. Damage to the system hardware, software, and/or operating environment requires total replacement / renovation of all impacted systems. The implementation of the Disaster Recovery Plan in a remote recovery site is required to restore Ex Libris cloud services to normal operation.

Disaster Recovery Strategy

DR Strategies for Minor & Major Disasters

Data Loss caused by Hardware or Software Failure

This section details the activities undertaken to restore data loss or corruption due to a minor or major disaster at the hardware and software level.

Root Cause Analysis

- A DR Team Engineer will perform troubleshooting to determine the direct cause of the data loss.
- In the event the loss is attributable to hardware failure, the DR Hardware Response Team will be notified.
- In the event the loss is attributable to software failure or human error, the DR Application Response Team will be notified.

Data Loss caused by Hardware Failure

- The virtualized instance of the customer’s hosted environment will be mounted from existing standby hardware that

has been preloaded with the appropriate operating system and administrative applications.

- The system vendor will be contacted with a request for emergency services.
- If required, data restoration will be performed from an onsite or offsite backup
- Hardware repair or replacement will be performed.
- Customer notification would be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

Data Loss caused by data corruption or application issues

- Software will be repaired or reinstallation will be performed.
- Data restoration will be performed from an onsite or offsite backup.
- Customer notification would be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

Service Disruption caused by hardware or facility event

This section details the activities undertaken for resumption of services due to a minor or major disaster at either the hardware or facilities level.

Root Cause Analysis

- A DR Team Engineer will perform problem determination activities to determine the direct cause of the interruption or loss of service.
- In the event the loss is attributable to hardware failure, either the DR Hardware Response Team or the facilities provider DR Operations Team will be notified (whichever is applicable).
- In the event the loss is attributable to software failure or human error, the DR Application Response Team will be notified.

Service Disruption caused by Facilities Provider Hardware Failure

- Facilities provider-owned resolution activities will be tracked by the Ex Libris engineer through completion.
- Hardware repair or replacement will be performed.
- Customer notification would be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

Service Disruption Due to Ex Libris' Cloud Services Hardware Failure

- The virtualized instance of the customer's hosted environment will be mounted from an existing standby hardware that has been preloaded with the appropriate OS and administrative applications.
- The system vendor will be contacted with a request for emergency service.
- Hardware repair or replacement will be performed.
- If required, all necessary software configurations will be performed on the repaired or replaced hardware.
- Customer notification would be updated at Ex Libris Status Portal (status.exlibrisgroup.com).

DR Strategy for Catastrophic Disaster

This section details the activities undertaken for restoration of cloud services due to catastrophic disaster at the facilities level:

- The BCP Team Leaders, in conjunction with the facilities provider, will perform an assessment of the extent of the facilities loss.
- In the event the primary facility will be out of service for an extended period of time (longer than 7 days), customer notification would be updated at Ex Libris Status Portal.

- An assessment of the viability of retrieving Ex Libris owned equipment from the disaster site will be performed.
- Simultaneously, a predetermined alternate facilities provider will be notified and engaged.
- Any hardware that can be retrieved will be reclaimed by Ex Libris for use in the designated recovery site.
- Procurement activities for replacement equipment to replace non-retrievable equipment will be initiated.
- A plan and timeline for implementation of the recovery site will be finalized and distributed to the Ex Libris customer stakeholders.
- The implementation plan will be executed.
- The Ex Libris and customer stakeholders will be notified of resumption of service at the alternative hosting facility.

Locate and Salvage Data and Equipment

Early efforts are targeted at protecting and preserving the salvageable computer and networking equipment (any hardware that can be retrieved will be reclaimed by Ex Libris for use in the Recovery Site). In particular, any backup storage media (hard drives, backup tapes) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

An inspection of the data center and telecommunication closets scene is done by BCP Team Leaders to estimate the amount of time required to put the salvageable equipment back into working order, providing there are adequate facilities to work with. A decision is then made whether to use a designated remote location where computing and networking capabilities can be temporarily restored until the primary site is available. If estimates from this process indicate that recovery at the original site will require more than 7 days, migration to the remote recovery site is initiated by notifying and engaging with a predetermined alternate facilities provider.

Systems and Data Recovery

Ex Libris will use salvageable equipment if possible. If equipment is damaged beyond repair, the Ex Libris Procurement Team will work with our vendors (listed in Appendix B) to expedite replacement equipment.

Data recovery is performed using backups retrieved from the disaster site from the offsite backup locations. Backups can take on various forms of media including hard drives and magnetic tapes. After identifying salvageable equipment, early data recovery efforts first focus on restoring the operating system(s) for each system. Next, mission critical system data is restored. After system data is restored, individual customer data is restored.

Move Back to Restored Primary Sites

If the recovery process has taken place at an alternate remote site, physical restoration of the primary data center will have begun. When the data center is ready for occupancy, the systems assembled at the alternate remote site are to be moved back to their permanent home.

This section outlines the logistical planning to be undertaken in order to transfer services back to the primary hosting site in the event that services needed to be moved to a designated recovery site to mitigate a catastrophic site disaster.

Operational readiness at the original primary site must be verified prior to the execution of this step. Once verified, the following steps will be initiated:

- Migration schedule availability at the facilities supplier
- Migration schedule availability with the customer
- Cloud Services preparation for migration
- Migration execution
- Systems Acceptance Test (SAT) and User Acceptance Test (UAT) completion
- Notice to Operations of migration

Plan Maintenance and Testing

Having a Business Continuity Plan is critical. But the plan will rapidly become obsolete if a workable procedure for maintaining the plan is not also developed and implemented. This section provides information about the maintenance procedures necessary to keep it up to date.

Business Continuity Coordinator (BCC)

The Business Continuity Coordinator has overall responsibility for the design, development, coordination, implementation, administration, training, awareness programs, and maintenance of the Business Continuity Plan. The BCC will follow the best practices established by the DRI International Professional Practices for Business Continuity Planners (see www.drii.org for the latest version).

In accordance with the DRII Professional Practices, the Business Continuity Coordinator has the following responsibilities:

- Provide BCP project coordination and management.
- Perform risk evaluation and mitigation as required.
- Develop and obtain approval for the Business Continuity Strategy (ies).
- Develop and implement the Business Continuity Plan.
- Develop, maintain, coordinate, exercise, and evaluate the BCP.

Business Continuity Plan Maintenance

The plan will be annually evaluated and updated. All portions of the plan will be reviewed by the Ex Libris COO and Cloud Engineering Director. If it is deemed that portions need to changed or be rewritten or reviewed by other cloud teams, the COO will assign that task to the appropriate team. In addition the plan will be tested on a regular basis and any faults will be corrected. The BCP Management Team has the responsibility of overseeing the individual components and files and ensuring that they meet standards consistent with the rest of the plan.

Exercising (Testing) the BCP

The Business Continuity Coordinator is responsible for conducting periodic exercises of the Business Continuity Plan using different methodologies (structured walk-through exercise, tactical exercise, and technical exercise for the BCP Team Leaders) or combination of these methodologies. A report will be submitted to the BCP Management Team after the completion of the exercise that will detail the success and/or failure of the exercise. A discussion surrounding any improvements to the plan will occur. Any revisions to the document based upon the results of the test and the discussion in management will be integrated into the document.

Appendix A : BCP & DR Team Contacts

The following list contains the relevant information for the Ex Libris Group DR Project Team leaders:

Name	Role	Mobile	Email
Ex Libris 24x7 hub	Ex Libris 24/7 Support, and communication	+ *-***-***-***	**********
**********	Ex Libris Chief Operating Officer	+*-***-***-****	**********
**********	Ex Libris Sr. Director of Cloud Engineering	+*-***-***-****	**********
**********	VP Cloud Services	+***-**-***-****	**********
**********	Chief Information Security Officer	+***-**-***-****	**********
**********	Privacy and Regulation Officer	+***-**-***-****	**********
**********	Cloud infrastructure Engineer	+***-**-***-****	**********
**********	Cloud Production Engineer	+***-**-***-****	**********
Hosted facility First Touch Response	Data center 24/7 Smart hands, Operations, and Support	+ *-***-***-***	**********
ISP, CDN	24/7 NOC	+ *-***-***-***	**********

* Masked to maintain privacy

Appendix B: Vendor Contact List

Below is the contact information for current main vendors of most components in this recovery plan.

This list will be updated for all vendors used by Ex Libris cloud services as it relates to disaster recovery efforts.

Vendor	Product	Support Number (regional)	Vendor Website
Cisco	Network Switches, Routers, Servers	+1 800 553 2447	http://www.cisco.com/

Vendor	Product	Support Number (regional)	Vendor Website
		+61 2 8446 7411 +32 2 704 5555	
Dell	Servers	1-800-624-9896 1800 394 7488 020 674 45 00	http://www.dell.com/
NetApp	Storage	888.463.8277 800.44.638277 800.800.80.800	http://www.netapp.com/
Nimble	Storage	1-877-364-6253 0-800-020-0730 800-852-3823	http://www.nimblestorage.com/
Juniper	Firewall	1-888-314-5822 0800 022 3531 001-800-2586-4737	http://www.juniper.net/
A10	Load Balancers	1-408-325-8676	http://www.a10networks.com/
Equinix	Data center facilities	1.866.378.4649 +31.(0).20.808.0015 800.852.3382	http://www.equinix.com/
Internap	IP & CDN	1+877.843.4662 00-800-0044-0055 001-800-0044-0055	http://www.internap.com/
Palo Alto	Anti-virus	US: (866) 898-9087 Int'l: +1 (408) 738-7799 EMEA +31 20 808 4600	http://www.paloaltonetworks.com/

Vendor	Product	Support Number (regional)	Vendor Website
		APAC: +65 3158 5600	
CyberArk	Access Control	US: 1-844-537-7700 EMEA: +44-203-728-7074 APAC: +65-6460-4254	https://www.cyberark.com/

Record of Changes

Type of Information	Document Data
Document Title:	Ex Libris Group Cloud Services Business Continuity Plan (BCP)
Document Owner:	Tomer Shemesh - Ex Libris Chief Information Security Officer (CISO).
Approved by:	Eyal Alkalay – Ex Libris Sr. Director of Cloud Engineering
Issued:	Apr 18 ,2014
Reviewed & Revised:	Apr 26 ,2018

Revision Control

Version Number	Nature of Change	Date Approved
1.0	Initial version	Apr 18 ,2014
1.1	Updated – Bar V	Apr 22 ,2014
1.2	Updated – Eyal A	Apr 23 ,2014
1.3	Review and Update- Tomer S	Feb 4 ,2015

Version Number	Nature of Change	Date Approved
1.4	Review and Update- Tomer S	Apr 12 ,2016
1.5	Review and Update- Tomer S	Jul 12 ,2017
1.6	Review and Update- Tomer S	Dec 14 ,2017
2.0	Review and Update- Tomer s	Apr 26 ,2018

Document Distribution and Review

The document owner will distribute this document to all approvers when it is first created and as changes or updates are made. This document will be reviewed and updated annually or upon written request by an approver or stakeholder. Questions or feedback about this document can be directed to the owner or a listed approver