Securing Next-Generation Library Services

An Ex Libris Alma Security Overview

ExLibris a ProQuest Company

CONFIDENTIAL INFORMATION

DISCLAIMER

TRADEMARKS

Document released: Month Year

Web address: http://www.exlibrisgroup.com

Table of Contents

Introduction

Information security has become an integral part of effective corporate governance, regulatory compliance, and risk assessment. A multiplicity of Internet-based hostile programs, such as viruses and password crackers, lay in wait to exploit any vulnerability, rendering information protection a domain that demands attentiveness, determination, and perseverance. In this context, libraries are a particularly attractive target, since they use high-speed Internet connectivity and run much of their business and many services online. Furthermore, libraries that are associated with educational institutions often hold sensitive patrons' data in their systems.

The Cloud Landscape

Cloud computing offers some major benefits:

- The system is accessible anywhere, anytime.
- The resources allocated for the customer's needs are flexible and scalable.
- The system is more environmentally friendly, because the customer uses only ready-made resources such as hardware and electricity, which are tailored to the customer's needs.
- The system is offered as an open platform that permits collaboration.
- Moving to the cloud allows information technology (IT) departments to shift their focus from worrying about constant server updates and other computing issues to concentrating on innovation and new initiatives.

Alongside the benefits of cloud computing are some vulnerabilities and threats that are derived from the nature of cloud-computing. According to the Cloud Security Alliance (CSA), the cloud, as an open platform, can be used by hackers or malicious insiders for staging attacks. Hence, cloud-based solutions can be subjected to new threats, such as account, service, and traffic hijacking.[1]

The Ex Libris Alma Security Model

Cloud security and confidentiality are top concerns with cloud computing and software-as-a-service (SaaS) architecture. Committed to providing its customers with the most secured and reliable environment, Ex Libris has developed a multi-tiered security model for Alma that covers all aspects of cloud-based systems. The security model and controls are based on

[1] Top Threats to Cloud Computing V1.0: *https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf*

renowned international protocols and standards and industry best practices, including ISO/IEC 27001:2013, ISO /IEC 27018:2014,ISO/IEC 22301:2012 and CSA Star Self-Assessment.

Ex Libris has received several security and privacy certifications, including ISO/IEC 27001:2013, ISO/IEC 27018:2014, ISO/IEC 22301:2012 and CSA Star Self-Assessment. The ISO/IEC 27018:2014 standard establishes commonly accepted control objectives, including controls and guidelines for protecting Personally Identifiable Information (PII) for the public cloud computing environment in accordance with the privacy principles in ISO/IEC 29100. The ISO/IEC 22301:2012 standard focuses exclusively on business continuity management (BCM).The CSA Star Self-Assessment provides transparency and quality assurance for Ex Libris cloud services. The ISO/IEC 27001:2013 standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).

Alma multi-dimensional security model defines the security controls that are applied to the various dimensions to address vulnerabilities, as illustrated in Figure 1. This paper elaborates on each of the security dimensions and the security means Alma makes use of.

Figure 1. Alma's multi-dimensional Security Approach

As part of the company's focus on security issues, Ex Libris employs a dedicated Security Officer who is the contact person for security issues and a Privacy and Regulation Officer for privacy and regulation issues and a dedicated security team along with a Cloud Services team that are responsible for the following tasks:

- Applying the security model to all system tiers
- Monitoring and analyzing the infrastructure for suspicious activities and potential threats
- Issuing periodic security and service level agreement (SLA) reports to Ex Libris management and customers
- Dynamically updating the security model and addressing new security threats

Another group, the Ex Libris security team, performs the following tasks, which are based on the Information Security Management System ISO/IEC 27001 standard:

- Examining the organization's information security risks, while mapping the related threats and vulnerabilities
- Designing and implementing a comprehensive series of information security controls and measures to answer underlying risks that are evaluated as unacceptable
- Adopting an ongoing management process to ensure that the controls taken meet the company's evolving security needs Ex Libris is committed to securing the information that our customer community stores in our systems. Each of the controls provided by Ex Libris as part of its multi-tiered security model is adhered to throughout the organization. The security model is constantly monitored and tested to maintain a high level of security, thus granting Ex Libris users—libraries and their patrons—peace of mind with respect to the privacy, confidentiality, integrity, and availability of their data.

Physical Security

Environmental Controls

A variety of physical and environmental controls are implemented at the Ex Libris data center facilities in order to make sure that only an authorized personal get access to the secured Ex Libris Data Center.

Multiple physical means are taken including:

- Physically locking of Alma servers inside the infrastructure in a designated area. In addition, another related physical control to ensure servers availability is the use of cooling systems by a separate air conditioning system, which keeps the climate at the desired temperature to prevent service outage.
- A fire suppression system protects the computing equipment and has built-in fire, water, and smoke detectors.
- The facilities have on-site generators, which serve as an alternative power source.

- A 24-hour video surveillance of all entrances and exits, lobbies, and ancillary rooms. The videos are recorded, monitored, and retained for later use.
- Biometric authentication is used as part of staff authentications and authorization process prior accessing the data center facility
- Uninterruptible Power Supply (UPS) systems and redundant backup diesel generators
- a robust HVAC system with minimum N+1 redundancy for all major equipment
- N+2 redundancy for chillers and Thermal energy storage
- Earthquake anchoring and bracing systems, flood controls, etc.

Physical Access Control

The data center physical security controls includes: 24x7x365 physical security, access is restricted to personnel with a business need to access the infrastructure, all physical access activities are logged and monitored, all doors (including server cages) secured with biometric hand geometry readers, CCTV digital camera coverage of the entire center with detailed surveillance and audit logs, and CCTV integrated with access.

In addition to the physical access authentication described above, all visitors need to be approved beforehand, and the approval is for a limited period of time. Visitors must be accompanied by an authorized employee throughout their visit. No one can access the facilities without signing a security log, being accompanied by an escort, and approval.

Infrastructure Security

Change Management

In order to prevent an unauthorized change in the cloud environment, and maintain the high level of service to Alma customers, Ex Libris has implemented change management procedures so that all activities are recorded, documented, scheduled, and approved. Every change in cloud production servers must follow the following procedure:

- planning stage – document, test procedure
- Approved cycle of the procedures, at least 4 eyes approval principle
- Coordination and notifications
- Execution in maintenance time

- Documentation

The Hub 24x7 NOC and Cloud teams are monitor and audit this process .

The Ex Libris Security Officer validates the procedure enforced and it is audited as part of the ISO audit and certification process that all security measures are in place.

Access Control System

In order to increase monitoring and enforce our strict access control policies,

Ex Libris utilizes Access Control system, a privileged account security solution that performs the following:

- The access control system is the only focal point through which access to the Ex Libris cloud servers can be made
- The access control system validates if the user is authorized to access the server.
- Throughout the user's activity on the server, the tool checks and enforces that only approved activity on the server is performed
- The access control system restricts access according to predefined user and policy restrictions
- Any session to a production server can only be made through the access control server (that is, from the authorized Ex Libris employee to the access control system and from the access control system to the server). In this way, the access channel itself is controlled
- All the data related to access rights, credentials, etc. are stored encrypted
- The predefined sensitive operation activity sessions are recorded and tracked for review

On a daily basis, the Ex Libris' Security Officer reviews a correlated audit and compliance report. Any suspicious activity, potential violations, or unauthorized access is handled immediately according to the Ex Libris Security response policy. These audit and compliance reports contain information that enables Ex Libris to track safe activities in order to meet audit requirements, including privileged accounts compliance status, entitlement reports, and activities logs.

Operating System Hardening

Operating systems used in the cloud are hardened according to best practices in the industry. Only services and components that are necessary to support the application stack are activated; the administrator user must always use a password, and only necessary ports in the firewall are open. Every new OS security fix is distributed to the entire cloud infrastructure.

Any device, including hypervisors, goes through a process that includes change management and a full QA process before implemented into Production, with bi-annual scans (SANS top 25) and annual penetration testing. Ex Libris verifies that these standards are followed through annual audit, penetration tests, and compliance reviews.

All components deployed for cloud architecture are based on a defined secure standard from the vendor and security best practices, and goes through a change control process that includes configuration, testing, and QA, before it is deployed in Production.

Security event log connections at the OS level include at least the following information:

- User identification
- Date and time of event
- Indication of success or failure
- Origin of event
- Identity of affected resource

All security event logs at the OS are analyzed, correlated, and evaluated daily.

Network Security

Firewalls

The Alma cloud has multiple firewalls installed to shield it from the growing number of attacks and prevent the loss of valuable customer data. The firewalls are redundant and configured to serve as perimeter firewalls to block ports and protocols as well identify and block malicious communication and attack attempts.

Network-Based Intrusion Detection and Prevention

The combination of an intrusion detection system (IDS) and intrusion prevention system (IPS) installed in the Alma cloud tracks all illegal activities. The Intrusion Prevention System provides end to end protection for the system and infrastructure with full network segregation and isolation from vulnerabilities and DoS/DDoS attack.

The system sends real-time alerts and proactively blocks communication once a suspicious attack is discovered. The system performs various activities on the network: log collection and

analysis from the various machines (firewalls, switches, and routers), file integrity checking, and rootkit detection.

Ex Libris uses a 24-hour security network operations center (NOC) to make sure that security-related issues are reported and handled as efficiently as possible.

Malware Prevention and Antivirus Scanning

Malicious activities, such as malware and phishing attacks, are considered serious threats that might lead to the compromising of customer data. To address these threats, Ex Libris performs manual and automatic antivirus scanning of the system storage.

Each file that is uploaded to and downloaded from the cloud is scanned by an antivirus engine.

Each vulnerability incident that is tracked is proactively neutralized and logged.

Secured Network Communication

Ex Libris encrypts all types of communications between the local institutions and Alma, using no less than 128 bit encryption key strength. This is accomplished using HTTPS, SFTP, or equivalent methods and covers all types of communications from staff browser secured communication to secured email server communication (Secured SMTP), secured file transfer (that is used for patron data load, integration with financial system etc.) using Secured FTP communication and more.

Application Security

Secured Development Life Cycle

System security starts at the very early stages of planning and design and continues with development methodology according to security best practices.

The development of Alma is made according to the industry Security Development Life Cycle (SDLC) best practice as described below:

Planning

During the planning stage, the security officer submits a report specifying the security requirements for all of the solution's components, such as the application, the database, and the client side.

To manage security issues optimally, the security officer uses various methods, such as access control, auditing, and monitoring.

Design and Development

The security officer verifies that the design and development of the product are based on the security guidelines. Other security issues are addressed by an additional security gap assessment document.

Implementation, Testing, and Documentation

Unit, integration, and system testing confirm that the security requirements were properly implemented. The requirements are documented and become standard policy.

Deployment and Maintenance

The security officer is responsible for identifying, managing, and minimizing security vulnerabilities. The security officer also performs on going security audits and reviews.

Monitoring and Protecting Against Common Web Vulnerabilities

The protection against common vulnerabilities is done at different levels. At the development level, our development teams follow security development best practices to avoid such vulnerabilities. In addition, we make use of security code review tools to help us identify any potential vulnerability at the development stage. Another layer that we make use of is vulnerability scanning that we perform on our application during testing and on the production environment. All of these scans are made in accordance with OWASP top vulnerabilities and best practices. Lastly, we make use of firewalls. Part of our short term roadmap plans include the use of WAF to protect against such vulnerabilities, should one still exist despite all of the measures taken as described above.

Continuous Monitoring of Security Controls

Ex Libris has implemented multi-tiered security audits on different levels: security checks on a daily basis, security reviews on a monthly basis, application security vulnerability assessment scans on a quarterly basis, as well as third-party patching on a quarterly basis and an annual scan of network vulnerabilities.

The ISO 27001 certification that Ex Libris passed successfully includes annual external audits to validate that all security measures and mitigations are in place.

OWASP Top 10

In order to make sure that Alma's security capabilities meet new and top security threats, the Alma code is tested and reviewed according to OWASP Top 10 security vulnerabilities. Alma security capabilities are constantly reviewed and updated in order to make sure top security threats are being covered and dealt.

Data Security

Data in Motion Encryption

With its distributed architecture, the SaaS model involves more data being in transit than in traditional architectures. For example, data is transferred between multiple physical machines in order to synchronize their images. For this reason, attacks that target data which is 'on the move', such as man-in-the-middle attacks, are serious threats in a SaaS model.

To address these threats, Alma utilizes SSL /TLS encryption (based on a commercial SSL/TLS certificate) using SHA encryption algorithm utilizing at least 2048 key strength, which creates an encrypted channel between the client desktop and the Web server and between the application server and the database server.

Data at Rest Encryption

In addition, patrons' personal data is stored by Alma also encrypted to prevent unauthorized access to it and can be read only by authorized staff members using Alma application.

The encryption and decryption of the information are performed in real time so that data at rest is always protected. Ex Libris uses a standard mechanism for handling the encryption keys. All encryption keys that are generated are random and are stored separately from the credential-

management zone. Encryption keys are never exposed in a clear form and are destroyed at the end of their designated period.

Data Isolation

Data isolation is defined based on either shared resources using firewall rules for network isolation, separate databases for database isolation, or separate files and permissions for files sharing isolation. As a multi-tenant cloud service, we also enforces strict data isolation to all layers of the application: user-interface branding isolation, storage isolation, and FTP-level isolation. In addition, our cloud service makes use of Oracle Virtual Private (VPD) in order to provide complete data isolation also at the database level. Finally the security penetration testing performed by an external security company validates that all isolations and segregations are in place.

Data Sanitization

Ex Libris has strict procedures and a unique policy for handling obsolete data based on the DoD 5220.22-M standard. These procedures are also applied if a customer decides to stop using Alma. Disks are destroyed once they are no longer needed. CDs that are no longer needed are destroyed by a CD/DVD data crusher or shredder. All storage devices that may need to be used again are cleaned by data wipe software.

Backup and Restore

Ex Libris maintains a well-developed backup plan consisting of multiple snapshots per day, including a full daily backup. The backups are made to a disk, a reliable backup media, and is stored in a remote secured location. This ensures that at any point in time, in case of a local disaster, Ex Libris has a secure copy of the data readily available. On a regular basis, Ex Libris performs system backups of application files, database files, and storage files. The privacy controls in practice at Ex Libris are enforced for all backup files. All backup files are retained for 10 weeks.

- On-site backup – Full backups of the OS platform, application, and customer data are performed at least daily (multiple snapshots are taken during the day for critical services/systems) using storage snapshot technology. The backups are kept for one week on-site on a separated set of disks. The snapshots are automatically mounted with specified access restrictions managed by the operating system in a specified set of directories that allows for an easy and immediate restore of the data at any time by Ex Libris authorized personnel.

- Off-site backup – Full backups of the OS platform, application, and customer data are performed daily using snap mirror technology over a dedicated, private secured network connection from the primary data center 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 restored to the main data center 24/7 by Ex Libris authorized personnel. The backups are kept at the off-site backup managed locations.

The restore procedures are tested on an ongoing monthly basis to ensure rapid and successful restoration in case of data loss. Additionally, a full copy of the data is maintained at a remote secured location.

Handling of File Uploads

Alma uses an open platform that enables the software to be integrated with remote systems. Some of the integrations use file-based data transmission between the applications. To minimize the vulnerabilities that can result from handling these files, Ex Libris has strict procedures for uploading files.

Each file that is uploaded undergoes integrity checks, is scanned for malicious content, and is checked against a whitelist of file extensions. The upload is done over a secure channel.

Sending/Receiving Customer Data

As a Cloud based SaaS solution, Scoped Data is sent or received electronically. All communication to the application are encrypted using SSL/TLS encryption (based on a commercial SSL certificate), which creates an encrypted channel between the user computer and the Ex Libris cloud-based service.

Data Retention for Customer Data

The customer is in full control of the data stored in the SaaS service and has responsibility to determine the retention requirements for the customer's data.

Accuracy of Customer Data

The customer is in full control of the data stored in the SaaS service and has responsibility to ensure accuracy and currency of their information

Identity and Access Control

Important aspect of prevention of unauthorized access to the systems is strong authentication method. Alma supported several user authentication methods that customer can choose from.

Secured LDAP Based Authentication

In this authentication method, Alma connects to the institutional LDAP server through a secured communication channel. The specific Alma roles of staff members maintain and managed in Alma, where the actual authentication of staff member is done by using the local LDAP. Upon login request, Alma communicates with the local LDAP and validates that the staff member ID is valid and authorized to login to Alma.

SAML Based SSO Authentication

Alma authentication architecture also supports single sign-on (SSO), which uses the enterprise identity provider authentication system. In this architecture, Alma delegates authentication to the customer's identity provider, whereby a circle of trust is built with the different domains. In this case (depending on the customer's identity provider being used), federation standards (based on the Security Assertions Markup Language [SAML] protocol) are applied.

Secured Application Based Authentication

Another authentication option supported by Alma is the use of Alma authentication mechanism to authenticate the staff members and store their passwords encrypted in Alma. The authentication is based on both Alma and the user browser side salting and hashing the user password at the browser side. Once Alma receives the hashed password from the browser, it compares it with its own hashed value. The entire authentication process is made using secured SSL communication channel.

In addition, Alma implements a security feature that locks out a user who attempts to log on more than a defined number of times—the maximum number of attempts (NOA). Alma also enforces strict password rules, which apply to both the operational team members and the application's users. Password rules include aging, length, combination, and reuse enforcement. All passwords are stored encrypted; using a one-way encryption method based on an industry-

standard hash algorithm; and only the application is able to compare the hashed and entered passwords.

Data Segregation

Since the privacy and confidentiality of its customers' data are the company's top priority, Ex Libris has developed extended authorization controls. The Alma authorization mechanism is based on the role-based access control (RBAC) model, which supports the segregation of duties. Segregation of duties is applied in order to minimize the risks and possibilities of misusing privileges. Users see only the menus and data that are derived from their roles and privileges. The system is constantly tested to ensure that users do not have multiple privileges that allow them to perform roles that conflict with other roles.

All access-control activities produce logs with enough information to meet auditing requirements and support usage charges. In addition, the access-control activities generate notifications to designated library staff to prevent users from setting up rogue accounts or otherwise modifying access entitlements.

Business Continuity

Alma is designed in accordance with the SaaS model. The system is based on multi-tenant architecture, in which all the resources are shared (Figure 2). This model enables Ex Libris to provide its customers with a fault-tolerant computing environment that includes dynamic resource allocation. This means that in case of one or more components failure, the system can still continue its normal operation.

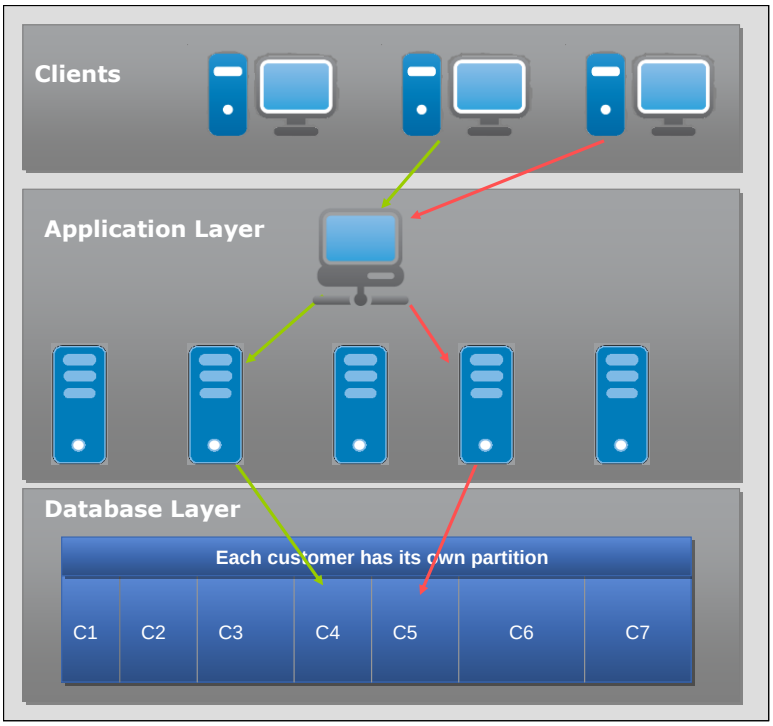


Figure 2. Alma's multi-tenancy model

Ex Libris maintains a comprehensive Business Continuity Plan for cloud services. This plan is tested at least annually. Detailed information can be found in the document, *Ex Libris Cloud Service BCP*.

Ex Libris has developed a high-availability solution to ensure that the system is resilient if business is disrupted. The solution applies to all components of the system and complies with the fundamental guidelines of business continuity: full redundancy, load balancing, and failover, as illustrated below. Each component in the system utilizes high availability capabilities: from the storage, database to the network routers, redundant firewalls as well as the utilization of multiple internet service providers to guarantee network access to the data center. This high availability architecture protects the system from one or more components' failures and offers high level of resiliency and business continuity.

Ex Libris is committed to high up time and availability. Ex Libris' standard SLA commitment is to deliver service availability of at least 99.5%, measured over any calendar year. Based on our experience with thousands of institutions deployed in our cloud environment, a number of which are large consortia, actual system availability is significantly higher. In addition, our standard SLA for responding to system down events is within one hour (in most cases our 24x7 HUB will identify a system down event even before system users). The cloud environment is monitored 24x7, with staff attending to any issues in real time. In order to achieve high availability, Ex Libris provides a redundant infrastructure with no single point of failure, and robust backup procedures in order to avoid data loss.

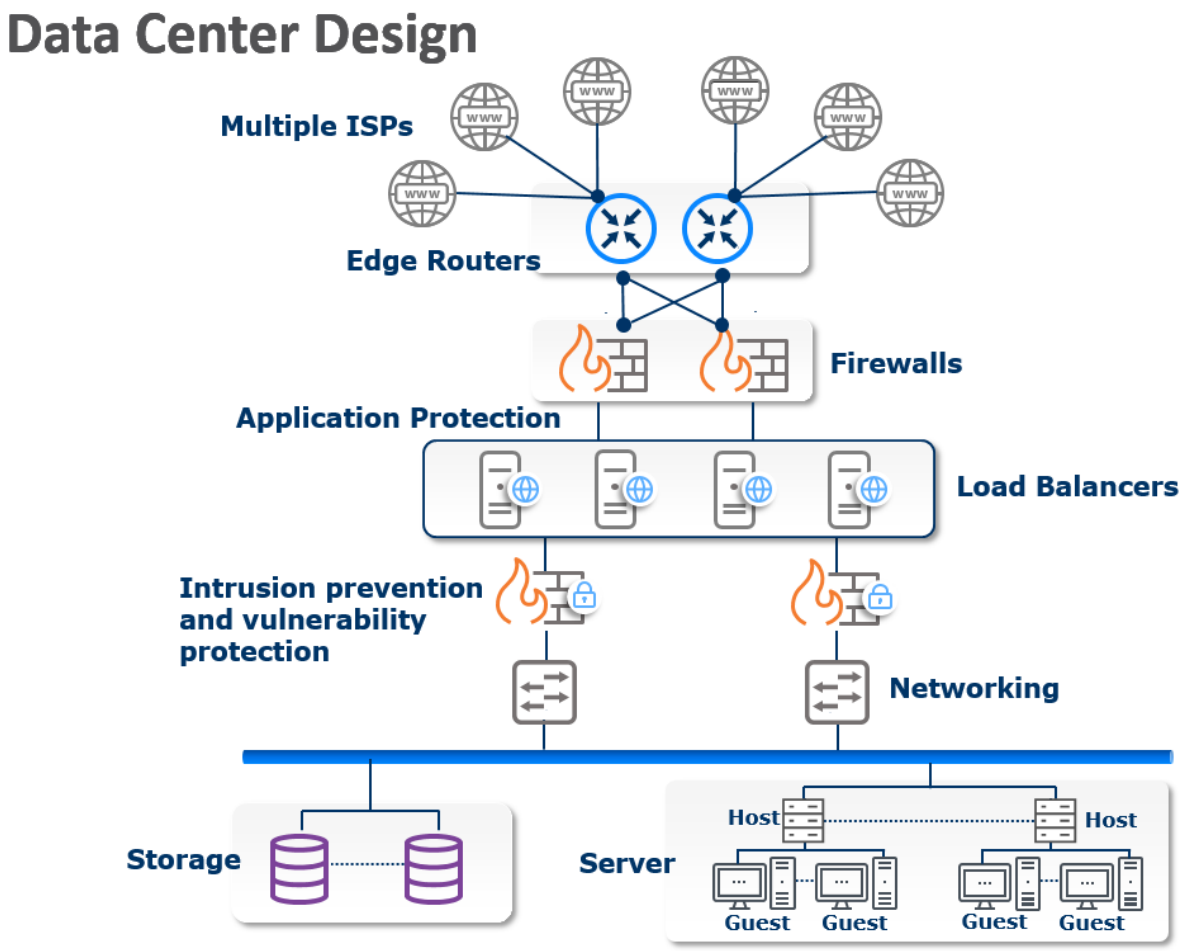
Minor issues and interruptions are addressed by our 24x7 HUB procedures, triggering events within a few minutes and lead to resolution by an event manager and senior engineers. The

BCP policy outlines the method of addressing larger events, which the Ex Libris cloud services group has classified disasters and emergencies into the following three levels – minor, major and catastrophic.

In the event of a major or catastrophic event, data recovery is performed using backups retrieved from the disaster site from the offsite backup locations. 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.

High-Availability Solution

Ex Libris has developed and designed a high-availability solution based on a No Single Point of Failure principle so that the system will be resilient in case business is disrupted. The solution applies to all components of the system and complies with the fundamental guidelines of business continuity: full redundancy, load balancing, and failover as illustrated in Figure 3 below. Each component in the system utilizes high availability capabilities: from the storage, database to the network routers, redundant firewalls as well as the utilization of multiple internet service providers to guarantee network access to the data center. This high availability architecture protects the system from one or more components' failures and offers high level of resiliency and business continuity.



Monitoring and Incident Management

Great emphasize is made on the on-going monitoring of Alma cloud environment. As a SaaS vendor, a great responsibility relies on the vendor's as the one that manages the entire solution environment.

Ex Libris' NOC provides 24x7 logging and monitoring for all logical network access to customer data and information asset usage and is audited by the Ex Libris Security Officer. Ex Libris monitoring consists of multi-layered, fully redundant systems that monitor the services inside and outside of the data center to validate that services are running at the highest possible performance levels.

Incident Management

Ex Libris has an Incident Response Policy. After Ex Libris determines that a security breach has occurred or that customer data has been compromised or accessed by an unauthorized person, Ex Libris notifies the customer as soon as reasonably practicable (and in any event, within 24 hours).

As part of the Ex Libris security incident response policy, Ex Libris commits to take prompt action to investigate the incident, mitigate any harm stemming from the incident, and take action intended to prevent any similar incidents from occurring, including, without limitation, the installation of appropriate patches or software fixes as soon as reasonably practical.

After Ex Libris has determined that a security breach has occurred or that customer data has been compromised or accessed by an unauthorized person, Ex Libris shall:

- Within 24 hours, or sooner if reasonably practical, notify the customer
- Take prompt action to investigate the incident and mitigate any harm flowing from the incident
- Assist the customer to make any required notifications to 3rd parties
- Take prompt action to prevent any similar incident from occurring, including, without limitation, the installation of appropriate patches or software fixes as soon as reasonably possible

Incident Response, Notification and Remediation

Ex Libris employs a dedicated incident-handling team that responds to security incidents and mitigates risks. The team uses monitoring and tracking tools and performs real-time analysis. Additionally, the team has clear procedures in place for communicating the incidents to any involved party and for handling escalations. Every incident is forwarded to the security officer for assessment and analysis.

Human Resources Security

At the end of the day, it is people that drive the business and the daily operation and according to security breaches statistics, many of vulnerabilities are result of human errors and insiders that tried to hack the system. Having the human factor in mind, Ex Libris adopted as part of its ISO 27001:2013 certification a strict procedure to certify staff to deal with its SaaS offering including monitoring procedures.

Prior to the employment of new staff by Ex Libris, candidates are subject to vetting and are required to sign confidentiality agreements. Background checks are performed for staff employed in critical roles who have direct access to customer production data, such as system administrators.

As part of our recruitment processes, staff undergo extensive background checks. The standard check includes S.C check, criminal history, employment verification, and reference checks, as well as additional checks dependent on business needs. Compliance with this procedure is audited as part of our ISO 27001:2013 certification.

Ex Libris realizes that the malicious activities of an insider could have an impact on the confidentiality, integrity, and availability of all types of data and has therefore formulated policies and procedures concerning the hiring of IT administrators or others with system access. Ex Libris has also formulated policies and procedures for the ongoing periodic evaluation of IT administrators or others with system access. User permissions are continuously updated and adjusted so that when a user's job no longer involves infrastructure management, his/her console access rights are immediately revoked. This process is enforced for any change of status or employee termination.

In addition to that, Ex Libris have set of Security and Privacy policies, procedures and guidelines for Ex Libris Employee that cover physical, account, data, corporate services, network and computer systems, applications services, and systems services.

Ex Libris incorporates the philosophy of “least privilege” and “need to know” principles for authentication, security requirements, separation, isolation, segregation, and security measures as part of operating procedures. Ex Libris’ ISO 27001:2013 certification confirms that these security practices are in place.

Those Security policies and procedures including using best practice standards in the industry for keeping confidentiality, privacy , business ethics, appropriate usage, and professional standards.

All employees are required to execute those policies and procedures. The security officer validates the enforcement and audit as part of ISO 27001:2013 security frameworks.

Security Awareness and Training

Ex Libris conducts privacy and security awareness training programs that are audited as part of ISO certification. The audit validates that all staff are trained in the areas of general information security secure code, protecting customer data and how to report any suspicious activity to the Ex Libris Security Officer.

Ex Libris has implemented security training and awareness annually as part of our employee life cycle processes to grant or remove permissions based on “least privilege” and “need to know" principles. Ex Libris passed the ISO 27001:2013 certification audit that validates training in personnel.

Compliance and Audit

Continuous Monitoring of Security Controls

Ex Libris performs multi-tiered security audits that include:

- security checks on a daily basis
- security reviews on a monthly basis
- application security vulnerability assessment scans on a quarterly basis
- third-party patching on a quarterly basis
- annual scan of network vulnerabilities

The ISO 27001 certification that Ex Libris passed successfully includes annual external audits to validate that all security measures and mitigations are in place.

Additionally, Ex Libris engages an independent security company that performs a security penetration test based on the OWASP Top 10 and SANS 25 best practices.

ISO Certification

Ex Libris is ISO 27001:2013 (information security standard) certified for all data centers, global operations, and application and development processes. The ISO 27001:2013 certification process requires that Ex Libris comply with of all Information Security Management System (ISMS) security measures and pass an annual compliance audit conducted by an independent third party audit firm. The ISO 27001:2013 audit process includes penetration testing, which is conducted by an independent third party security company at least annually.

ISO/IEC 27018:2014

Ex Libris is ISO 27018:2014 (Protection of PII) and earned the certification in February 2016. ISO 27018:2014 defines the controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) for the public cloud computing environment.

ISO/IEC 22301:2012

Ex Libris is certified with 22301:2012 that focuses exclusively on business continuity management (BCM). The ISO 22301 is a comprehensive standard that represents the highest level of commitment to business continuity and disaster preparedness. By achieving ISO 22301 certification, Ex Libris continues to demonstrate its focus on high availability and business continuity, as well as the company's commitment to providing customers with a reliable and highly secure SaaS environment.

ISO/IEC 27001:2013

Ex Libris was certified by the International Standards Organization (ISO) for ISO 27001:2013 which is the most rigorous global security standard that sets out requirements for an Information Security Management System, including Examining the organization's information security risks, while mapping the related threats and vulnerabilities , Designing and implementing a comprehensive series of information security controls and measures and Adopting an ongoing management process to ensure that the controls taken meet the company's evolving security needs.

To achieve the certification, a company must show it has a systematic and ongoing approach to managing sensitive company and customer information and demonstrates that Ex Libris' cloud services security is in line with world-class standards, ensuring it meets the needs of its security conscious customers.

The certification includes Ex Libris' data centers in Europe and APAC as the result of an in-depth audit of the centers' control objectives and control activities, including controls over information technology and all other related processes.

SSAE16 SOC1 Compliant

The Ex Libris data centers are SSAE16 SOC compliant, following a process in which an in-depth audit of the centers' control objectives and control activities, including controls over information technology and all other related processes were taken by auditors.

Ex Libris Privacy Policy

Ex Libris privacy policies can be found at http://www.exlibrisgroup.com/category/Privacy.

Risk Management and Risk Assessment

Ex Libris performs annual risk assessments using an independent Security consultant, based on the principles detailed in NIST Special Publication 800-30, defined as the following:

- Agree the company's key business processes and the technology assets that support them
- Identify threats to these processes and where assets are vulnerable to these threats
- Rate the base risk level of each threat and assess the controls in place to mitigate the risks
- Provide control recommendations and evaluate the residual risk after control recommendations are implemented

The annual risk assessments includes interviews with stakeholders and key company personnel to define and review the security risks levels and implement security measurements.

Ex Libris Risk Management is reviewed and approved as part of ISO 27001:2013 Certification process.