Diligent

Diligent Trust Site

Diligent Security Overview

Every person, team, and organization using Diligent applications and services expects their data to be secure, available, and handled according to strict confidentiality and privacy principles at all times—and we understand how important this is.

We have built our global business on the trust our customers place in our ability to safeguard their data, and continue to maintain that trust through our security and compliance initiatives and culture of continuous improvement.

Our commitment

We are committed to providing a robust and secure service that protects our customers' data.

We provide our service to customers and we also use it ourselves—storing our corporate data in our products. We do so knowing that our platform is built upon industry-standard security technology, refined principles and practices, and ongoing investments in security training, testing, independent audits, expert consulting, and advanced tooling.

Site Contents

Security Environment and Principles

We have a dedicated Security department consisting of over a dozen security professionals focusing on product security, security operations, incident response, risk management, and compliance. The Security Team is overseen by a Chief Information Security Officer (CISO).

Our multi-layered security environment follows the principles of least privilege, separation of duties, defense in depth, and usability. Customers have ownership of user access controls and manage the entire customer data life cycle in deciding:

- what data goes into their system
- how long it should be retained
- what data should be deleted
- who can access the data

Benefits

Our products are designed to take advantage of the efficiency and accessibility of a cloud-based, software as a service (SaaS) delivery model. Our SaaS solutions provide organizations with independence and agility along with a low and predictable total cost of ownership.

Deployment decreases from months to days

Our services are designed with the philosophy of "convention over customization," enabling our customers to immediately leverage configurable "out of the box" functionality vs. relying on heavy customization, complexity, and the overhead costs it brings.

Time to value with a SaaS delivery model is significantly lower than with on-premise solutions. This means that implementation times are typically measured in days vs. weeks or months for other solutions.

Powerful and continuously improving functionality

Our services are enhanced with robust functionality, and product improvements are continuously delivered so that you do not need to wait for long release cycles or internal IT resources to use the latest product version. This ensures that the user interface and product features remain modern and up-to-date with business demands.

Low TCO and predictable costs

The SaaS delivery model takes away large upfront capital or implementation costs, making the ongoing costs much lower and more predictable than legacy on-premise alternatives.

No dependence on IT resources and in-house IT service costs

Our services do not require new hardware, software, or IT support for initial implementation or ongoing maintenance. Our customers can selfmanage

and focus on using the application for their business function, leaving the complexities of administrative management, application

operation, and maintenance of the infrastructure to our global operations team.

Beautiful and easy-to-use interface

Our services are designed with usability as a top priority. Elegant, interactive, web-based interfaces mean that organizations can start using the

software quickly.

Integrated risk and control analytics and monitoring

Our products integrate seamlessly, providing an end-to-end technology solution for all aspects of Corporate Governance from a single vendor.

Accessible anywhere and from any device

Our services are accessible to employees spread across multiple locations worldwide from their PC, smartphone, or tablet.

Frequently asked questions

What type of security and controls are in place for data centers and sub service organizations?

We use a combination of global cloud service providers and colocation data centers to host our public and private cloud SaaS offerings. The data centers provide physical and logical security controls and are compliant with various certifications and third-party attestations, including but not limited to: ISO 27001, PCI DSS Level 1,

SSAE-16/ISAE 3402 SOC 1 (previously SAS 70 Type II), SOC 2 & 3, and HIPAA. Colocation data centers operate at Tier 3 level. Below are examples of these controls:

- User Access
- Logical Security
- Data Handling
- Physical Security
- Vulnerability Management
- Change Management
- Data Integrity, Availability, and Redundancy
- Incident Handling

These controls ensure facility and equipment safeguards for areas such as multi-factor access controls, electronic surveillance, intrusion detection systems, and environmental safeguards.

We review the certifications and third-party attestations provided by our sub service providers on an on-going basis to attest the services being provided and supplement complementary elements to our internal controls.

Is a SOC audit report available?

Yes, we have current SOC 2 reports for specific products prepared by third-party auditors. The reports are comprehensive assessments of the internal controls and information security related to our service.

Upon request and subject to customer's execution of our standard non-disclosure agreement (NDA), we will provide a copy of a current SOC 2 report.

Do you conduct vulnerability assessments and penetration tests?

In addition to internal security testing, we use third-party independent penetration testing to assess our service for security vulnerabilities. These tests are performed by an organizations specializing in software security, and are used to probe our environment for vulnerabilities and OWASP Top 10 web application risks, such as:

- cross-site scripting
- SQL Injection
- session and cookie management
- API abuse
- denial of service

We ensure exploitable vulnerabilities are resolved in a timely fashion based on severity and impact. Subject to an NDA, we can provide a copy of the most recent penetration test.

What type of security and controls does Diligent have in place?

Our system control environment is designed to provide confidentiality, availability, and integrity for our SaaS offerings. Controls that are audited at least annually under SSAE-18 include:

- Data Protection
- Access Control/Logical
- Access Change Management
- Data Security
- Backup and Recovery
- Incident Management

These controls and supporting policies provide us and our customers with operational assurance.

Where will my data be stored?

Systems that rely on our IaaS provider are available in regions in the United States, Canada, Europe, Australia, South Africa, South America, and Asia. Systems that rely on our colocation data centers are available in United States, United Kingdom, Canada, Germany, and Australia to provide options for where data is stored and to help our customers comply with data privacy location requirements.

How do you protect Personally Identifiable Information (PII)?

PII is limited by our customer subscription agreements, sub service organization agreements, corresponding controls, and segregation built into our SaaS design. This ensures that any PII is isolated and protected in the system and that each customer has access to its data only.

Who will have ownership of my data?

You will continue to retain all rights over your data and we will not use your data except for the purpose of providing the services in your subscription.

Reporting Security Concerns

We recognize that the decision to store data in a cloud-based platform raises important questions about security. If you have any questions or concerns about the security, privacy, or integrity of your data, contact our support team.

To report a specific vulnerability, see our https://www.diligent.com/vulnerability-disclosure/

Compliance Resources

Introduction to Compliance at Diligent

Diligent's Security Program is governed based on NIST Cybersecurity Framework and Diligent follows ISO/IEC 27001 standards to keep information assets secure by implementing an Information Security Management System (ISMS). This provides a systematic approach for managing people, processes, and IT systems. Diligent's ISMS is ISO/IEC 27001:2013, 27017:2015, and 27018:2019 certified.

Certifications and Attestations

Access all Diligent's auditor-issued reports, certifications, accreditations, and other third-party attestations.

Title	Reporting Period	Category	Description	Product
ISO 27001:2013 Certification	January 1, 2022 to December 31, 2022	Public Cloud	This certification, issued by an independent third-party auditor, validates that Diligent's Public Cloud product complies with the ISO 27001 internationally- recognized standard for security management best practices and comprehensive security controls following the ISO 27002 best practice guidance.	HighBond
SOC 2 Type 2		Public Cloud	The SOC 2 Type 2 report evaluates the Diligent Public Cloud product controls that meet the criteria for security and availability in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Criteria. This is our most recent SOC 2 report. SOC reports are audits performed over a period of time and do not expire. Our auditors perform our SOC audits twice a year over a period of 6 months.	HighBond
ISO 27001:2013, 27017:2015, and 27018:2019	April 19, 2022 to April 10, 2025 Cert No. 1469286-10	Co-location	This certification, issued by an independent third-party auditor, validates that Diligent's Public Cloud product complies with the ISO 27001 internationally- recognized standard for security management best practices and comprehensive security controls following the ISO 27002 best practice guidance.	Diligent Boards, Entities, Diligent Equity, Secure File Share/Secure Workflow, BoardEffect

SOC 2 Type 2	Mar 1, 2021 to Feb 28, 2022	Co-location	The SOC 2 Type 2 report evaluates Diligent Product controls that meet the criteria for security and availability in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Criteria. This is our most recent SOC 2 report. SOC reports are audits performed over a period of time and do not expire. Our auditors perform our SOC audits annually over a period of 12 months.	Diligent Boards, Entities, Diligent Equity, Secure File Share/Secure Workflow, BoardEffect
SOC 1 Type 2	Mar 1, 2021 to Feb 28, 2022	Co-location	The SOC 1 Type 2 report evaluates controls relevant to customers internal controls over financial reporting. This is our most recent SOC 1 report. SOC reports are audits performed over a period of time and do not expire. Our auditors perform our SOC audits annually over a period of 12 months.	Diligent Boards, BoardEffect
HIPAA/HITECH	Feb 28, 2022	Co-location	The HIPAA/HITECH attestation evaluates the information security program for conformity to the applicable implementation specifications within the HIPAA Security Rule and the HITECH Breach Notification Requirements as described in Part 164 of CFR 45, as of the date shown.	Diligent Boards, Entities, BoardEffect

Privacy

Processing Personal Data

The GDPR applies to the processing of EU personal data wholly or partly by automated means, as well as to non-automated processing, if it is part of a structured filing system. “Processing” covers a wide range of activities, including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

We understand that customers who use our platform and related services may wish to process EU personal data in connection with such use and will be required to comply with the GDPR. In such cases, Diligent will be the processor or sub-processor of such EU personal data.

For more info about Diligent’s Privacy Policy, please visit: https://www.diligent.com/privacy

Security of Personal Data

Security is the crux of all data protection. At Diligent, we are continually monitoring and improving our security and compliance capabilities for all of our customers globally. We maintain GDPR security compliance through our annual compliance reports and our robust information security program. Ahead of GDPR, we assessed our technical and organizational controls specific to the protection of personal data and have updated security processes where needed.

Data Processing Addendum for Customers

For customers who process EU and/or UK personal data in connection with their use of Diligent’s products and related services, Diligent offers a Data Processing Addendum to ensure compliance with EU and UK GDPR obligation to have a written contract in place with Diligent as a data processor. The Diligent Data Processing Addendum is available at https://www.diligent.com/data-processing-addendum.

Additional information on Diligent's global processing operations is available at https://www.diligent.com/privacy. For customers using only our on- premises products, all data in these products remains on the customer's systems. Diligent does not access or process any of that data.

Our Data Protection Officer can be contacted at: privacy@diligent.com.

Vendor Compliance with GDPR

Our vendor management program ensures that any vendors who are sub-processors of EU personal data will adhere to the same security standards as Diligent and are also GDPR compliant. Diligent enters into a written data processing agreement with each of our sub-processors to ensure such compliance and to ensure that any transfers of EU personal data are made only in accordance with GDPR.

For a list of Diligent Group Companies and Sub-processors, see https://www.diligent.com/gdpr-subscription/.

Policies, Processes, and Practices

Information security policies and processes form the backbone of our information security program. Diligent's security policies set the tone and direction for the organization, assign and delegate roles and responsibilities for information security, establish control objectives, and demonstrate commitment and account ability to all constituents, including employees, business partners, and customers.

Information Security Policies and Processes

Our services are supported by various operational and security policies, standards, and procedures related to:

- Personnel Security
- Acceptable Use
- Data Protection
- Risk Management
- Access Control
- Cloud Computing
- Physical Security
- Asset Management
- Third Party Management
- Network and System Secure Design
- Security Incident Response
- Vulnerability Management
- Change Management
- Capacity Management
- Secure Software Development
- Business Continuity and Disaster Recovery

Physical and environmental security

Our corporate headquarters building is located in a shared physical facility. The building's entrance is kept locked during non-business hours, and is further protected by a security guard service. Security cameras are visibly placed in high traffic or sensitive locations.

Diligent office doors require badge access prior to granting entry. All employees, contractors, and visitors must wear a visible badge at all time. All doors are alarmed and will alert our vendor and the police if a disturbance is detected. Physical access is audited every quarter, however, no customer data is stored at our facility.

Logical security

We use a principle of least privilege for internal administration. Employees who require administrative access must be requested via a ticketing system. The request requires the approval of senior management before access is granted.

Administrative access to all applications is granted to employees only based on user job responsibilities. Access to all production system and internal applications is removed immediately upon employee termination or contractor contract termination. On a quarterly basis, a review of access rights is conducted.

Incident management

We have a robust Incident Response Plan to promptly and effectively manage incidents that impact the system environment. This plan is in place to both minimize potential damages that could result from a data breach and to ensure that parties affected by the data breach are properly informed and educated on how to protect themselves.

The Security Incident Response Team (SIRT) is

responsible for responding, managing, and conducting security investigations, including all aspects of communication such as deciding how, when, and to whom the findings shall be reported.

Breach notifications

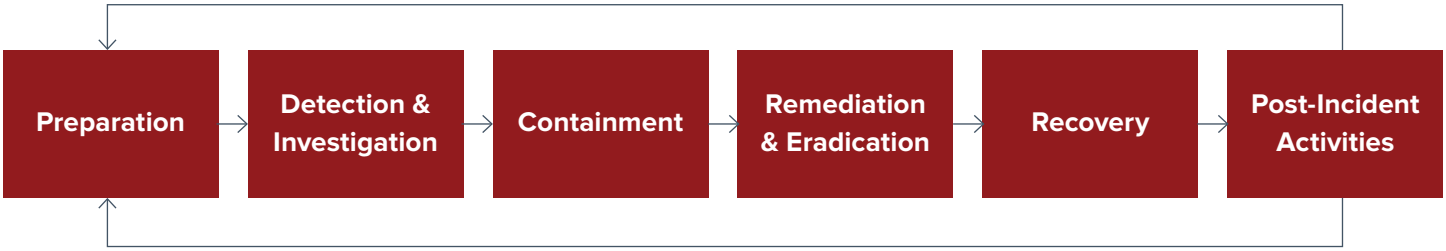
In the case of an incident, notifications are made in a timely manner to affected parties. The notification will include:

- A brief description of the incident, including the nature of the breach and the date it occurred
- A description of the general type(s) of data that were involved in the breach (not an individual's specific information)
- An explanation of what we are doing to investigate the breach, mitigate its negative effects, and prevent future incidents

Incident management workflow

The lifecycle for a security breach incident at Diligent

The Diligent incident management lifecycle encompasses six phases: preparation, detection and investigation, containment, remediation and eradication, recovery, and post-incident activities.



Preparation

Preparation includes those activities that enable the SIRT to respond to an incident: policies, tools, procedures, training, effective governance, and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

Detection and Investigation

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident.

We monitor and investigate all events and reports of suspicious or unexpected activity, and track them in an internal ticketing system.

Investigation is the phase where SIRT personnel identify and determine the priority, scope, and root cause of the incident. The Investigations phase should include the completion of an "Incident Log". The incident log can be used during the following phases of the incident, to keep track of all incident activities. This will be a reference aid during the incident closedown and can also provide information for the lessons learned phase.

Containment

Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication. All evidence will be handled in accordance with local evidence handling procedures and legal requirements.

Remediation and Eradication

Remediation is the post-incident repair and recovery of affected systems and or data, communication and instruction to affected parties, and analysis that confirms the threat has been contained. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

Recovery

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" into future response activities and training.

Post-Incident Activities

Post incident activities within the recovery stage include "Lessons Learned." Lessons Learned allows SIRT to identify any weaknesses in the plan and the supporting policy and or process and to put in place remedial actions to mitigate any further such incident.

During lesson learned, the SIRT will review the incident and examine all associated artifacts to identify any root cause. Lessons learned are documented and used to improve the plan.

Secure Software Development Life Cycle (SSDLC)

At all phases in the application development process, security is a top priority.

At Diligent, we build security into our software. Secure coding best practices are strictly followed. Common application layer vulnerabilities, including all OWASP Top 10 vulnerabilities, are explicitly addressed at all stages of the SDLC using industry standard counter-measures, such as explicit sanitization of all user input, use of parameterized queries, and use of secure libraries.

All code changes are controlled and approved, and must go through strict peer review and Quality Assurance (QA) testing prior to production deployment.

Development and testing

We employ industry-leading development practices such as pair programming and code review, as well as continuous integration tools to perform automated testing, including static code analysis for security.

Multiple staging environments have been established to facilitate manual and automated testing. Additionally, a formalized and independent QA function has been established to perform structured testing when a feature, bug fix, or higher risk change is to be introduced into our environment.

As an agile development shop, we maintain processes and tools to roll back changes in case problems arise from a production deployment.

Program management and DevOps

Program management is the responsibility of our DevOps and Production Operations teams. These groups maintain the servers (provisioning, backups, OS updates and patches, logging, and monitoring) and oversee the deployment of all changes from our Development (R&D) team into production, ensuring that our change management process has been followed.

DevOps and R&D work closely together to ensure the quality of our software service, but have separate responsibilities.

Segregation of duties

We have procedures, controls, and monitoring in place to ensure that a separation of duties exist between the define, design, built, test, and deploy phases of the software lifecycle.

We also use 3rd party monitoring for development, test, and production to detect run-time errors and monitor performance so multiple stakeholders are informed on deploy or error.

Workstation and laptop security controls

To maintain the security and integrity of our endpoints and data, the following key controls are implemented for all laptops and workstations in the Development environment:

- Full-disk encryption
- Restricted privileged accounts
- Managed detection and remediation (MDR) and endpoint detection and response (EDR)
- Standardized password authentication requirements
- VPN access
- Secure source code management with remote backups

Application code repository

We maintain a source code repository exclusively for source code management. The source code repository is a complete copy of the source code (including all version history).

The redundant nature of our source code repository significantly reduces risk to system availability from loss of source code. This repository is backed up on a regular basis.

Change management

Management has developed policies and procedures to control and manage changes to production systems.

We use segregated development, test, and production environments. All program changes are tested in a development environment, a continuous integration environment, and then formally accepted in a staging environment prior to being deployed in the production environment.

The deployment system has the capability to roll back any deployed changes so that even in the event an issue is encountered after deployment, the production application may be returned to a stable state quickly and efficiently.

Emergency change management

Emergency changes require the same testing and approval process as a standard change request. However, these activities may be performed and documented retroactive to the migration of the change to production, in order to make sure the production issue is resolved as quickly as possible.

Customer issues

Customer issues may be reported to Diligent Service by phone or support tickets. For details, see https://www.diligent.com/support/

The person receiving the request will attempt to immediately address the issue or route the issue to the appropriate person and document the resolution procedures.

Customer experience issues may also be identified automatically through application layer errors. When an error occurs in an application, a programmatic notification is made which automatically generates an e-mail notification. Once the notification is received, the ticket is used to track resolution to the error.

Penetration testing

In addition to internal security testing, we use 3rd party independent penetration testing to check the Diligent services for security vulnerabilities.

These tests are performed by an organization specializing in software security, and are used to probe the environment for vulnerabilities, such as cross-site scripting, SQL Injection, session and cookie management.

We ensure exploitable vulnerabilities are resolved in a timely basis based on severity and impact. A copy of the most recent penetration test report can be provided, subject to a non-disclosure agreement (NDA).

Web scans and testing

We use an independent 3rd party security provider to perform web application scanning and automated security testing. Vulnerability scans are performed to identify security flaws on all applications prior to a production release.

Any findings are escalated immediately and resolved in a timely fashion.

Security area	Description
Port discovery	Identifies and maps open ports across the production network.
Network services vulnerability scan	Discovers, identifies, and monitors network devices, finds rogue devices, or identifies unauthorized services.
Network discovery	Interrogates each service on every available port to determine exactly what software is running and how it is configured matching to the vulnerability knowledge base for launching of service-specific tests.
Web applications vulnerability scan	Checks all HTTP services and virtual domains for the existence of potentially dangerous modules, configuration settings, CGIs, and other scripts, as well as default-installed files. The website is then "deep crawled" including flash-embedded links and password-protected pages, to find forms and other potentially dangerous interactive elements. These are then exercised in specific ways to disclose any application-level vulnerabilities, such as code revelation, cross-site scripting, and SQL injection.

Terminating subscriptions

When you choose to terminate your subscription, we will extend access to the system for an additional 30 days to copy or extract any data you wish to retain. Once you have extracted your data, you have the full ability and responsibility to delete any or all of your remaining data in the system.

Upon written request, Diligent will destroy the customer system and all data content after the extract process. If 90 days has passed without written request to destroy the customer system, Diligent reserves the right to destroy the customer system to regain system resources.

For product specific terms, see https://www.diligent.com/governance-cloud-terms-conditions/.

Availability and Recovery

Diligent is committed to delivering a world-class customer experience.

Our SaaS solutions are designed using architectural best practices, such as:

- request load balancing
- resilient system design
- job isolation
- DDoS protection

We actively monitor our solutions for availability and performance to a 99.5%+ average uptime.

Identifying and resolving performance issues is a key part of providing high value SaaS based subscription to our customers. Furthermore, it is a top priority of Diligent that we provide responsive and effective customer support.

To access current system status page please visit:

https://diligent.statuspage.io/

https://status.highbond.com/

Data redundancy

All regional equipment is fully redundant and data is replicated or backed-up to alternate regional locations in case of failure. In addition to this real-time redundancy, we back up all customer data.

As long as your subscription is active, your data will be backed up.

Event monitoring

All product systems are monitored 24/7 for security and availability. In the event of any service interruption, alerts are delivered via e-mail, text message, and phone call to system administrators and management.

Security and performance are monitored using sophisticated third-party monitoring tools. Security and performance requirements are reviewed on a weekly basis and any issues noted that potentially impact customers are documented and resolved.

Disaster Recovery

We maintain a disaster recovery plan. While the customer impact of a physical or environmental threat to our corporate headquarters is considered low, Diligent personnel's safety and availability is mission critical.

Data center recovery procedures

All equipment at the data centers is fully redundant.

In addition to this real-time redundancy, we back up all system data, including field data and attached encrypted documents that are stored in customer accounts within each respective region.

Security Controls and Data Protection

Our security program is founded on the controls we have built into our services to protect customer data.

Security Controls Mission Statement

Confidentiality and integrity of customer data is our most important mission. We make all commercially and professionally reasonable efforts to maintain the highest levels of each, as customers would expect from us and themselves.

We regularly assess risk, monitor our controls, evaluate potential threats, and use this information to update our controls framework from policies and procedures to encryption protocols.

Security Controls and Data Protection Documentation

Product	Content	Link
Diligent Boards	Security Controls Overview	Diligent Boards Security Controls
Diligent Boards	Data Regions and Privacy Overview	Diligent Boards Data Regions and Privacy
HighBond	Security Controls Overview	HighBond Security Controls
HighBond	Data Regions and Privacy Overview	HighBond Data Regions and Privacy

HighBond Security Controls

HighBond security is founded on the controls we have built into our service to protect customer data. We regularly assess risk, monitor our controls, evaluate potential threats, and use this information to update our controls framework from policies and procedures to encryption protocols.

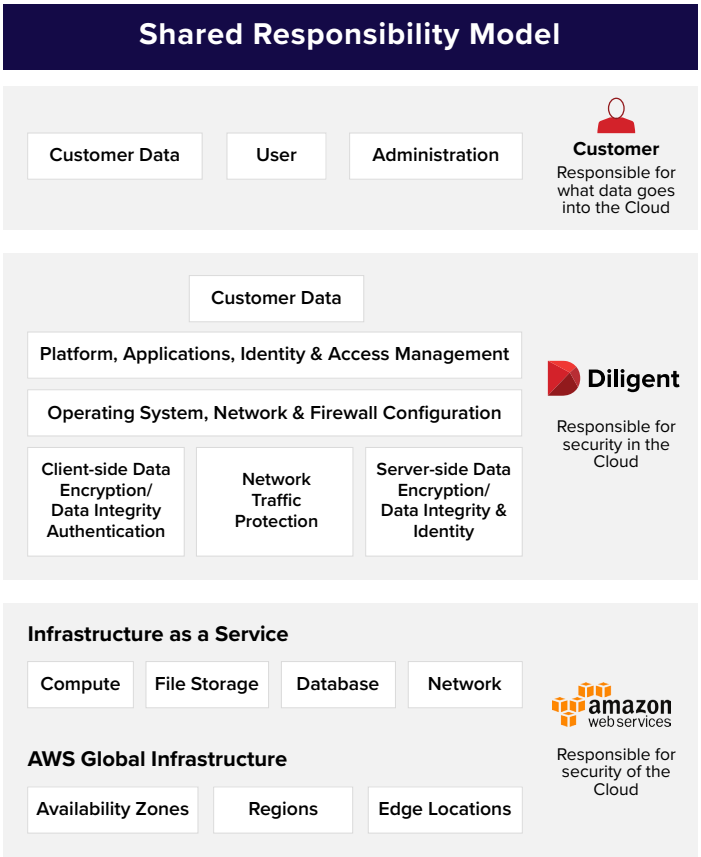
The type of data stored in our system commonly includes:

- risks, controls, and policies related to the organization or public sector entity at both a strategic or enterprise level and process or
- location level
- testing of design and effectiveness of risks, controls, and policies
- exceptions and issues related to the testing
- integrating relevant data analytics related to transactional data sampling or monitoring.

Shared Responsibility Model

Diligent manages the overall application infrastructure and our customers manage the end-user security and access control to their individual system. This is known as the Shared Responsibility Model, which is comprised of:

- Customer responsibility
- Diligent responsibility
- Amazon Web Service (AWS) responsibility



Customer Responsibility

Customers share the responsibility of not only keeping their data secure, but also complying with applicable regulatory or privacy laws. Our customers have full ownership of their user access controls and manage their entire data lifecycle from deciding what data goes into the system, how long it should be retained, what data should be deleted, and whom can access the data.

Customer environment access

Our customers should have controls in place to restrict access to the individuals to whom account access is required. Controls should include approving individuals for access to accounts prior to setting up users in the system and revoking users' log-in credentials when user access is no longer required or if user authentication credentials or other sensitive information has been compromised.

HighBond includes several capabilities to assist customers in their responsibility to manage end-user system access, including the ability to:

- Enforce strong passwords
- Configure password expiry
- Configure session timeout
- Configure SSO (Single-Sign On) via SAML 2.0
- Lock user accounts after multiple failed log-ins
- Easily delete or suspend user accounts
- Specifically identify permissible user IP addresses
- Use activity tracking to log access and system use

Diligent Responsibility

In addition to the physical and hardware security that Amazon provides, we also have a robust information security environment to ensure that the confidentiality, integrity and availability of customer data meets our high standards and our customers' high expectations.

Amazon Web Services (AWS) responsibility

Amazon is the largest vendor of data storage and computing on the planet, and they are responsible for the physical facility as well as the physical infrastructure of server hardware, networking, and related services for the HighBond service and hosting customer data.

Data Encryption

We provide strong encryption of all data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security) protocol supporting only the strongest encryption algorithms, including AES (Advanced Encryption Standard) with up to 256-bit key lengths. Encryption at rest is achieved by leveraging AWS storage encryption, using AWS KMS to create and store the 256-bit AES encryption keys.

About encryption

By using TLS version 1.2, an encrypted communication channel between the end-user web browser and the HighBond service is established, ensuring the confidentiality and integrity of all data transmissions from end-to-end.

The AES encryption algorithm is widely recognized and approved by organizations worldwide as an industry standard in government, military, and commercial applications.

AES-256 bit TLS encryption is supported on most browsers. If your browser does not support AES-256 bit TLS encryption, you will not be able to access the HighBond service and all related components.

All emails from our platform are transmitted via TLS-encrypted channels, when available. If the recipient's email server does not support TLS, emails are delivered over the default unencrypted connection.

Hashing function

If and when customers choose to publish data to Results for evidence as part of control testing, or for further review as part of risk mitigation, ACL Analytics and Analytics Exchange both include a hashing function for customer end-users to apply to any sensitive data fields, such as:

- patient records
- social security identifiers
- credit card numbers
- bank or mortgage account numbers
- payroll
- criminal activity

The hashing feature enables customers to cryptographically protect any sensitive data fields that are being uploaded to our service. Hashed values are protected by a cryptographic one-way function that cannot be reversed, keeping sensitive data confidential at rest and during further processing.

Passwords

User passwords are never stored. A strong cryptographic algorithm is used to generate irreversible strings known as password hashes. The stored hashes are without any value to an adversary even if obtained. The algorithm uses a unique long random value known as a salt, which is different for each user and ensures protection against attacks based on pre-computation of password hashes.

Password expiry

Password expiry is a security feature that limits unauthorized access to our service. If you are using password expiry, consider the following:

- Account Admins can enable password expiry under **Settings > Update Organization** in Launchpad.
- Password expiry is configured as the number of days between password changes.
- Note: The minimum duration supported for password expiry is 7 days. There is no maximum duration.
- If your password expires, one or more organizations you belong to have enabled password expiry.
- Your password expiry is based on the shortest expiry length of all the organizations you belong to.
- You will receive a notice in Launchpad one week prior to your password expiring.
- If your password expires, you will need to reset your password to sign in to Launchpad.

Password complexity

Our service includes a security setting that determines whether passwords meet complexity requirements. Complexity requirements are enforced when you change or reset your password in Launchpad.

Passwords must meet the following requirements:

- Passwords must be a minimum of 8 characters in length
- Passwords must include at least one lower case, one upper case, and one numeric character.
- Note: Passwords may contain special characters.
- You cannot re-use any of your last five passwords as your new password.

Password attempts

When signing in to our platform or generating a token to use in another application, you have up to five attempts to enter your password.

After five attempts, reCAPTCHA displays. reCAPTCHA is a service that protects websites from spam and abuse, and requires you to enter a series of characters or numbers to prove you are human.

Session expiry

A session is a period of activity between a user logging in and out of an application. Sessions are global to all HighBond SaaS modules, which means you use the same login session whether you are in Strategy, Projects, Results, or Reports. Your session expires if you are inactive for the duration of time set by an Account Admin.

Note: Session expiry does not apply to the mobile app, ACL Analytics, or Analytics Exchange.

When a new organization is created, the default session timeout is set to 60 minutes. If users have access to more than one organization, their session will expire as per the shortest session expiration time limit set across all their organizations.

If you are using session expiry, consider the following:

- Account Admins can enable session expiry under **Settings > Update Organization** in Launchpad.
- Session expiry is calculated by the number of minutes that a browser session remains inactive.
- The minimum duration supported for session expiry is 15 minutes and the maximum is 30 days.
- You can have multiple tabs open at one time in one browser as each tab or window belonging to the same browser on the same
- machine shares the session.
- You can use a maximum of two concurrent sessions in different browsers. If you log in from a third browser, the oldest session is expired.
- You can log in with either the same user or different users on different browsers or machines, and logging out of one will not log you out
- of the others.
- Your session expiry is based on the shortest expiry length of all the organizations you belong to.

IP Restrictions

IP restrictions allows organizations to configure one or more IP (Internet Protocol) addresses or IP address ranges from which a user may access the organization. IP restrictions may be used as an additional factor in multi-factor authentication, in addition to password credentials, to ensure only authorized users access the organization.

IP restrictions only impacts our applications when they interact with Cloud data, including:

- Exporting results from Results to ACL Analytics
- Importing results from ACL Analytics to Results
- Using scripts to export results from Analytics Exchange to Results
- Publishing results from Add-In for Excel to Results
- Importing tables from Projects to ACL Analytics
- Checking in or checking out sections in the mobile app or Projects client
- Uploading Excel worksheets from ACL Add-In for Excel to Projects

If you are using IP restrictions, consider the following:

- Account Admins can configure IP restrictions under **Settings > Update Organization** in Launchpad.
  Note: In order to prevent Accounts Admins from locking themselves out of our service, Account Admins are unable to configure an IP address that does not comply with their current IP address.
- If the IP allow list has any IP addresses or IP address ranges defined, only users whose IP addresses match the IP allow list may access the organization.
- All users accessing Cloud data within a specific organization are subject to IP restrictions.
- Users belonging to multiple organizations must comply only with the IP allow list of the organization they are currently accessing.
- If an IP allow list is enabled, users on mobile devices or public networks with dynamic IP addresses cannot comply with their organization's IP allow list.
  Tip: To comply with your organization's IP allowlist, you can connect to your organization's VPN (Virtual Private Network) to access our service on your laptop or mobile device.

Role-based access control

Roles define the types of permissions a user has in accessing cloud data. Permissions can include tasks such as managing settings, and adding, viewing, editing, or deleting data. A user can have varying roles in different modules.

Accountability

You are accountable to provision access to all of your licensed users via a designated Account Admin role, and in doing so, determine which users get access and to which level of access is required by business need and applicable compliance regulations.

Administering user access

Depending on how your organization manage logical access, you can use a centralized approach and assign your IT Department as Account Admin allowing them to administer overall user access.

Alternatively, you can use a more decentralized approach where the leadership of the respective assurance buying center(s) can administer access control through user application roles dictated that comply with IT or regulatory security requirements.

Obtaining our IaaS sub-service provider's SOC 2 reports

You can access AWS's latest audit reports and compliance information from https://aws.amazon.com/artifact/. AWS also provides additional security information and a compliance roadmap at the following locations:

- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/services-in-scope/

Based on the standard agreement all SaaS vendors have with Amazon, we cannot provide these reports directly to you. However, we will help you with information for obtaining them directly from Amazon. If you would like to obtain any of the AWS compliance reports, especially their SOC 2, please request instructions from your Diligent Account Executive.

HighBond Data Regions and Privacy

Our service is provided from four regions in order to give our customers options for where their data is stored, and to enable them to comply with data privacy location requirements.

Physical data storage

Data is stored and replicated across state-of-the-art data centers operated by Amazon Web Services (AWS).

Regional data storage

Upon system setup, your data in the platform is stored in the data center associated with your region based on the address listed in your Order Form. However you may choose an alternative storage region to suit your physical, legal, security, or performance needs. All data is encrypted during transmission and at rest within the regional data storage facility.

Our system is provided from the following regions:

- North America (US)
- North America (Canada)
- Europe (Germany)
- Asia Pacific (Singapore)
- Asia Pacific (Australia)
- South America (Brazil)
- Africa (South Africa)
- GovCloud (US Federal)
- GovCloud (US SLED)

All customer data, including data in backups, are stored exclusively in the single hosting region.

Exceptions

Some personally identifiable information in your licensed user profiles may be transferred to the United States region, including:

- First Name
- Last Name
- Email Address

Data Redundancy

All regional equipment is fully redundant and data is replicated or backed-up to alternate regional locations in case of failure.

In addition to this real-time redundancy, we back up all customer data, including field data and attached documents that are stored in your account within the system.

A full backup of the entire system database is run hourly, daily, and weekly for a one-year period, for the purpose of restoring data integrity due to systemic or database failure, but not for the purpose of restoring user deleted data.

As long as your subscription is active, your data will be backed up.

Data Availability

The maximum acceptable length of downtime for the service is 24 hours, even in the event of a disaster. The system recovery plan is tested to ensure this target can be met.

The maximum acceptable length of data loss is currently considered to be one hour, even in the event of disaster. Therefore, backup intervals are configured to allow for loss of customer data of one hour or less, depending on the time of system failure.

Data Retention

The system keeps all active or archived customer data continually when you have an active subscription, unless you choose to delete the data. You can determine:

- your own data retention controls for your active system
- the period for the retention of your data
- when you want to permanently delete data

System settings include the ability for designated system administrators to configure a time period after which archived project data is automatically and permanently deleted, but also allows the same on an ad hoc manual basis.

The vast majority of customers with active subscriptions rely on us to retain their data. However, you may choose to extract data for your own offline records as a secondary measure for data retention.

Note: As long as your subscription is active, this step is redundant and not necessary. As an example, if you maintain an active subscription for ten years, you will have ten years of data within the system (unless you choose to delete it).

Extracting or backing up data

There are several ways customers (authorized managers or administrators) can extract data at any time:

- Project reports can be saved to your network in PDF or Excel format.
- Entire projects can be extracted in a single compressed zip file, containing all system reports, native attachments, and an activity log for the audit trail.
- The reporting application can be used to extract customer data in a variety of formats, including comma delimited, Excel, Word, or PDF, among other options.

Customers are responsible for ensuring that only appropriate users are accessing their system and are authorized to do so.

We perform backups of customer data for the purpose of restoring data integrity due to systemic or database failure, including field data and attached documents that are stored in your account within the system on an hourly, daily, and weekly basis for a one-year period.

Migrating data from another system

Migrating data from one customer data center to another can be a complex process. Although there is no automated process available, customers can:

- Hire a Diligent consultant to perform the migration tasks for their organization
- Perform the migration themselves by completing the procedure below

Most customers do not migrate in-progress projects. Best practice is to leave in-progress projects in the existing source system and start new projects in the new system.

Data Privacy

Customer data is considered confidential information and is handled securely by Diligent personnel. Customer data is never copied to assets outside the production environment, including employee laptops.

Any troubleshooting that needs to be performed on customer data is performed in the customer's environment. When Diligent personnel need access to

a customer environment, a ticket is generated indicating that Support accessed the instance, why the interaction was necessary, and what work was performed.

Actions by Diligent personnel on a customer's system are limited to resolving the customer needs, and nothing more. Once a customer is satisfied with the result, and the ticket is closed, access is removed.

We collect only the minimum personally identifiable information necessary from your licensed users for purposes of account set-up, access to product resources, and system administration.

Data ownership

Customers own their data completely and are responsible for setting retention spans and for deleting unwanted content during the subscribed service and up to 30 days after termination or expiry of their subscription.

Customers have a responsibility of ensuring their data is in compliance with applicable policies, regulations, and laws, and Diligent has the responsibility of ensuring the platform hosting customer data is secure.

Diligent Boards Security Controls

Diligent security is founded on the controls we have built into our service to protect customer data. We regularly assess risk, monitor our controls, evaluate potential threats, and use this information to update our controls framework from policies and procedures to encryption protocols.

Diligent Boards is part of a suite of tools that can be used to form a Modern Governance strategy. Modern governance solutions bring together historically disparate tools into one secure product suite. Board materials, voting and resolutions, evaluations, collaboration tools, document sharing, committee intelligence, candidate search, entity management – all these tools and features work together to enable seamless management and reporting.

Shared Responsibility Model

We manage the overall application infrastructure and our customers manage the end-user security and access control to their individual sites. This is known as the Shared Responsibility Model, which is comprised of:

- Customer responsibility
- Diligent responsibility

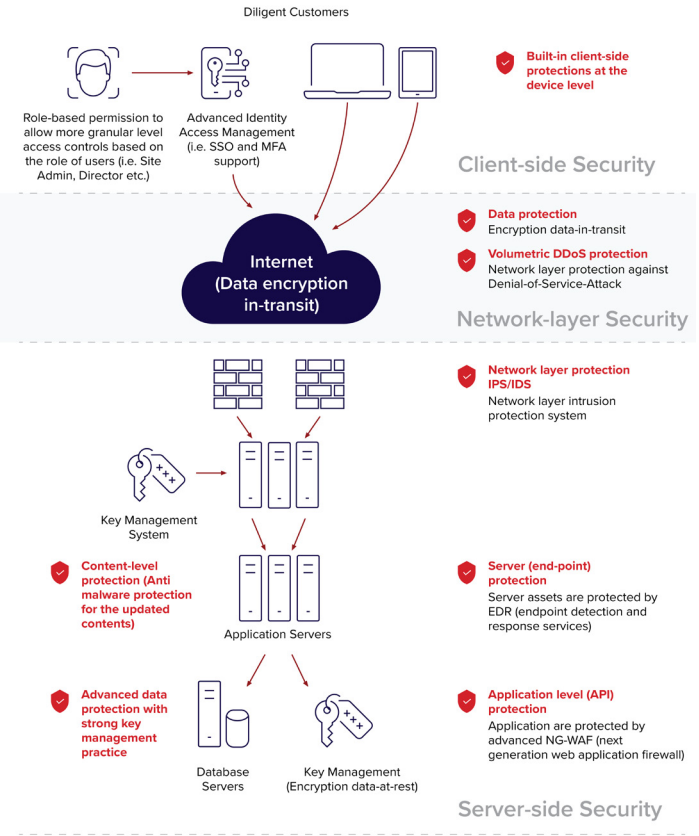
Customer Responsibility

Customers share the responsibility of not only keeping their data secure, but also complying with applicable regulatory or privacy laws. Our customers have ownership of their user access controls and manage their entire data lifecycle from deciding what data goes into the system, how long it should be retained, what data should be deleted, and whom can access the data.

Diligent Responsibility

Diligent is responsible for the physical facility as well as the physical infrastructure of server hardware, networking, and related services for the service and hosting customer data.

In addition to the physical security and infrastructure, we also have a robust information security environment to ensure that the confidentiality, integrity, and availability of customer data meets our high standards and our customers' high expectations.



Data Encryption

We provide strong encryption of all data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security) 1.2 protocol. Public Key Infrastructure (PKI) utilizes 2048-bit RSA Public/Private key pairs and SHA-2 for hashing.

Encryption at rest is achieved using AES utilizing Cipher Block Chaining (CBC) with a key length of 256 bits and a random initialization vector (IV). Data protection keys are managed on a per-customer basis at a minimum, with a two-key system and document-level encryption. The master encryption key is never stored in plain text and use of the customer master key to decrypt data protection keys is restricted to a Key Management Service (KMS) using a FIPS 140-2 L3 Hardware Security Module. Secrets are managed using industry-standard HSM devices.

Any data downloaded to a user's device is encrypted by the app using an offline data protection key. This encrypts the data with AES encryption. This is in addition to any encryption provided by the device's OS.

Identity and Access Management

Authentication

Authentication is performed by an authentication service that stores the passwords in hashed form only. Username and password are required by default and the password policy is configurable by the customer.

After a set number of incorrect login attempts, user accounts are locked out of the system.

SSO / Federated Identity

The Diligent Boards Web App and iOS App support login using client identity providers. This allows customers to sign into Boards with their own identity provider, as long as it uses a supported protocol.

Currently ADFS, Azure AD, and Okta are supported via SAML 2.0. Customer can leverage federated integration to support their own SSO (single sign on) or other strong authentication methods such as adaptive or 2FA authentications based on customer's internal security policy.

Multifactor Authentication (MFA)

Boards users can be configured to require MFA for authentication. The second factor is dependent on the application's platform. When accessing the web client, the user will require an SMS code, while accessing the mobile apps will require a certificate to be installed on the device. This certificate is implemented via the Device Authorization feature.

Device Authorization

Device Authorization provides a 2FA solution that is compatible with the offline functionality offered by the Boards mobile applications. This feature associates a user with a specific device via a certificate installed on the device, and restricts the user's access to Diligent Boards from that specific device. By restricting access to specific devices, customer organizations can prevent access from unknown and untrusted devices providing additional control of access rights and access locations. Device level authorization controls are also available, please contact Diligent CSM for details.

Authorization

Authorization in the Diligent platform is by determined the client and set by our customer success teams. This process applies to both direct and federated identity authentication to the application.

Diligent Boards employs a role-based access control (RBAC) model. The role-based permissions in Diligent Boards support both standardized roles and granular permissions per user. Privileges such as exporting materials can be disabled.

Session Expiry

- User Inactivity Timeout – Closes all windows and logs user out after specified amount of time.
- Inactive Session Timeout – Timeout period after last server request. Requires re-authentication to resume access.
- Maximum Server Session Duration – Forces reauthentication periodically according to a specified timeframe.

Platform Specific Considerations

On all platforms, Diligent Boards is designed to protect itself and data in the platform using secure design techniques and the available security resources of each platform. However, there are additional considerations outside of the controls available in Diligent client apps that can further strengthen the platform's security.

Enterprise Mobility Management/Mobile Device Management

Diligent Boards can be configured to disable certain features. While the Diligent Boards mobile apps contains some features typically included in EMM/MDM software, implementing an actual MDM solution to enforce a security policy for the device adds another layer of control especially for email, social networking, and printing.

Customers cannot distribute the iOS app from a private enterprise app store.

Device Passcodes

Requiring the use of a passcode, and preferably a strong passcode, is a first line defense in mitigating stolen devices or devices that may be accessed by unauthorized individuals.

Apple Devices

Apple allows users to track, find, and wipe their missing Apple devices when Find My iPhone is turned on.

Diligent Boards Web Client

The web interface code is written in industry-standard programming languages and supported by top-tier web services and web hosting. Most modern standards-compliant browsers are supported.

The following controls protect the web client:

- Boards Web is developed in accordance with Diligent's Software Development Lifecycle (SDLC). The program adheres to secure coding practices and guidance from OWASP SAMM (Software Assurance Maturity Model).
- Development follow guidance from OWASP to code protections against the OWASP top 10 most critical web application security risks, which includes attacks such as Cross-Site Scripting (XSS) and SQL Injection.
- No plug-ins or ActiveX Controls are needed in the web browser.
- Session information is stored as short-lived bearer tokens. The access token is randomly generated and hashed.
- Boards Web has configurable inactivity timeouts and a maximum session timeout. The timeouts fully terminate the session. Boards Web communicates securely with the Boards platform using HTTPS via TLS 1.2.
- Boards Web utilizes a third-party Runtime Application Self-Protection (RASP) product. The product protects against reverse engineering, IP theft, and tamping threats.
- Diligent regularly involves a specialist third-party to perform manual application penetration testing for Boards Web, including against the OWASP Top 10.

Diligent Boards for iOS

Code Obfuscation

This security strategy intentionally complicates the code base in order to prevent reverse engineering or other compromises to the underlying structure of Diligent Boards for iOS. By protecting the underlying programming language of Diligent Boards for iOS, code obfuscation acts as an additional defense against outsiders maliciously uncovering the methodology behind our security, encryption and data transfer practices.

Jailbreak Protection

The iOS App contains jailbreak detection code that will prevent the Diligent Boards App from running on devices that have been jailbroken. A number of jailbreak detection techniques are used ranging from process forking to detection of certain files and modules that are not normally present within iOS.

Touch ID/Face ID

If enabled, Diligent Boards utilizes Apple's proprietary fingerprint-reading technology "Touch ID" to allow users to sign in. Face ID replaces Touch ID thumbprint

identification functionality on most iPhone devices, as these devices no longer have a home button or fingerprint reader. Face ID is currently present on iPhone and iPad Pro devices.

App Transitions

Screen Security prevents Diligent Boards previews from appearing in the app switcher.

Data Backup Protection

Diligent Products contain controls to ensure that application data is not backed up to iTunes or iCloud.

Logging, Monitoring, and Alerting

Logging

The Diligent Platform includes a security-auditing framework that is designed to record any changes that are made to security settings, or information that could affect security. Auditing is automatically enabled for all clients, and the audit database is available for the duration of the customer's relationship with Diligent. All administrative functions are logged.

Monitoring

Diligent uses a security information and event management (SIEM) system to provide a data analysis function that enhances the ability to detect and respond to security incidents in a timely manner. The SIEM ingests logs from applications, servers, and other infrastructure components that form the Boards production environments, acting as a central repository of aggregated logs, allowing Diligent to monitor all system access, VPN access, privilege escalation (successful and failed attempts), and end-point protection, etc. The SIEM is managed by Diligent's Security Operations team using alerts and dashboards.

Only Diligent has access to SIEM logs. Customer related application logs must be manually requested and are provided in CSV format. There is no functionality to export customer application logs into the customer' SIEM.

Alerting

Role Change Notification

If an email address is nominated by an Authorized Representative, all notification emails associated with user role changes will be sent to this address.

Account Change Notification

If an email address is nominated by an Authorized Representative, all notification emails associated with user email, security question, and password updates, will be sent to this address.

Account Lockout Notification

If an email address is nominated by an Authorized Representative, all notifications relating to a user account lockout will be sent to this address.

Diligent Boards Data Regions and Privacy

Diligent Boards utilizes colocation data center services in the United States, United Kingdom, Canada, Germany, and Australia. Diligent owns and operates the infrastructure and the colocation vendors provide Tier 3 redundant utilities and environmental controls, as well as physical security controls.

Diligent infrastructure resides in its own dedicated, locked cage in the data center.

Data Center Physical Security

The colocation data centers feature the following security controls: Man-trap entry, onsite security officers, PIN and card readers, biometric readers, CCTV surveillance, and motion detection. Security systems have a dedicated uninterruptible power supply, plus backup power generation. Access by Diligent staff requires registration with the data center, prearranged visit ticket, and 2FA to enter the data center and equipment cage. Access to the facilities is reviewed annually.

The colocation data centers feature the following operational controls: redundant power feeds, UPS systems, backup generator, fire detection and suppression equipment, leak detection systems, and redundant HVAC systems.

Infrastructure

At the infrastructure perimeter are redundant firewalls with integrated Intrusion Detection/Prevention System (IDS/IPS). All connections into the application environment terminate on reverse proxy appliances which provide load balancing and redundancy. These appliances also segment the service tiers and restrict ports and protocols to only those required for the application.

Data movement among different networks segments inside of data centers are controlled by network firewalls by implementing application specific policies. Servers within the environment are protected by both signature-based and heuristic-based end-point protection tools. Data storage utilizes a scalable high-performance Storage Area Network (SAN). All data uploaded is continuously replicated to a secondary data center to allow for business continuity and disaster recovery.

Both infrastructure environments are continuously monitored for uptime, performance, security, and capacity. Monitoring is performed by Diligent's 24/7 Operations Team using logging, automated alerts, and dashboards.

Availability

Production infrastructure is implemented with many high availability features including clustered servers for each application component, load balancing among the components, and real-time application and infrastructure monitoring.

The redundant and modular design of the system also allows Diligent to perform most maintenance tasks without interrupting the service.

Web Application Firewall (WAF)

Diligent's application servers are protected by a next generation web application firewall (NG-WAF) to automatically detect and prevent OWASP top 10 attacks such as SQL Injection and Cross Site Scripting (XSS), as well as other malicious activities, including Path Traversal, Denial of Service, Malicious bots, API Abuse, and more.

Distributed Denial-of-Service (DDoS) Protection

DDoS protections are in place to protect the most critical assets based on risk assessments.

Backups and Disaster Recovery

Diligent has a documented Business Continuity and Disaster Recovery Plan. The plan includes a Disaster Recovery Site for production and corporate functionality, provisions for alternate work locations, assigned roles and responsibilities, provisions for pandemic/mass absenteeism via geographically remote sites, and customer notifications of a Disaster Recovery situation. The plan is reviewed and tested annually.

The backup schedule consists of daily differential backups and monthly full backups. Primary and secondary data center databases are kept in sync through disk-level replication. In addition to replication, customer data is backed up at the primary data center and then replicated to the secondary data center.

All backup data is encrypted and stored online at the data centers. Backups are kept for 60 days. No tape or other media is used, and no third- party storage providers are used.

Data Availability

The maximum acceptable length of downtime for the service is four hours, even in the event of a disaster. The system recovery plan is tested to ensure this target can be met.

The maximum acceptable length of data loss is currently considered to be four hours, even in the event of disaster. Therefore, backup intervals are configured to allow for loss of customer data of four hours or less, depending on the time of system failure.

Data Privacy

Customer data is considered confidential information and is handled securely by Diligent personnel. Customer data is never copied to assets outside the production environment, including employee laptops.

Any troubleshooting that needs to be performed on customer data is performed in the customer's environment. When Diligent personnel need access to a customer environment, a ticket is generated indicating that the Customer has authorizing and enabling Support to access the instance, why the interaction was necessary, and what work was performed.

Actions by Diligent personnel on a customer's system are limited to resolving the customer needs, and nothing more as the Customer is responsible for granting the authorization to access Customer material. Once a customer is satisfied with the result, and the ticket is closed, access is removed.

We collect only the minimum personally identifiable information necessary from your licensed users for purposes of account set-up, access to product resources, and system administration.

Data Retention

Boards client data is retained for the duration of the service contract. Aside from the contract, data retention is controlled by the customer. Customers can delete data from the database at their discretion. At the termination of the contract, the customer's database will be deleted on the production servers and backups will be removed promptly.

Diligent can assist customers with downloading their data in PDF format before the end of the contract.

Data Destruction

At termination of contract, Diligent ensures that the customer database, and any backups, are rendered unrecoverable and securely removed from storage.

Diligent will provide customer with confirmation of their site's deletion.

Data Jurisdiction

Customers can choose from a selection of countries to have their data hosted in. Hosting environments are physically and logically separated. Each environment is provisioned within a single country, consisting of a primary and secondary data center. There is no mechanism or configuration to replicate data to another hosting environment in a different country.

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS provider, serving more than one million users from over 25,000 organizations around the globe. Our modern GRC platform ensures boards, executives and other leaders have a holistic, integrated view of audit, risk, information security, ethics and compliance across the organization. Diligent brings technology, insights and confidence to leaders so they can build more effective, equitable and successful organizations.