AUDITBOARD CONTRACTS

FREQUENTLY ASKED QUESTIONS

(For information purposes only; this FAQ does not form part of any contract document.)

Thank you for reviewing AuditBoard's contracts for AuditBoard's cloud platform software-as-a-service. As you review the attached documents, we hope this FAQ will help you better understand what is being purchased and how AuditBoard's cloud service model works.

1. What is my company purchasing?

AuditBoard provides a fully functional enterprise cloud software-as-a-service through the web and browser app using a genuine one-to-many cloud delivery model. The platform is updated, and the data is backed up by AuditBoard. Similar to Salesforce and Workday, all AuditBoard customers are on the same version of the AuditBoard platform. AuditBoard provides its software on a single code line and on the same operational infrastructure, using the same security and support operations for all our customers.

2. How is AuditBoard's cloud service different from installed, on-premise software?

AuditBoard's cloud-based software is a true one-to-many business model. By contrast, on-premise software providers offer a customizable model, where each customer is treated differently — essentially an outsourced hosting of installed software. AuditBoard's business model allows for a more cost-effective delivery of solutions by ensuring that all customers are always using the most recent version of the software, which enables our customers to receive the latest features and security updates while avoiding costly and disruptive upgrades. Additionally, it avoids the heavy costs associated with the purchase and set up of physical hardware for a traditional on-prem solution.

3. How does AuditBoard protect its customers' data?

Protecting the security and privacy of our customers' data is a top priority for AuditBoard. AuditBoard defines customer data as the electronic data or information submitted by a customer, or on behalf of a customer, to the service platform. AuditBoard treats all customer data with the highest level of sensitivity and provides equal protection to safeguard personal and non-personal customer data. All customer data is encrypted before being stored in a logically segregated customer tenant within a secured data center. The customer remains in control of the data and is responsible for determining appropriate data access and use for the parties to which it authorizes use of the service.

4. Data Security:

AuditBoard's security program uses controls described in AuditBoard's Security, Privacy, and Architecture Documentation and AuditBoard's most recent SOC 2 report and ISO certification. AuditBoard provides customers with objective evidence that it is maintaining its security controls through our independently audited SOC Type II audits and ISO 27001 certification, which are made available to customers upon written request. That way, our customers have independent verification of and visibility into the security controls protecting their customer data, and AuditBoard contractually commits that such controls will not be materially decreased or degraded.

5. Why can't my security exhibits be attached to the contract?

AuditBoard maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data, protect against security threats and data breaches, and prevent unauthorized access to customer data. As a true one-to-many cloud provider, AuditBoard operates a single-tenant platform where all customers share a single version of the software with logical segregation between customers. All of our security controls are designed from the ground up for a cloud environment and a consistent set of security controls is applied to our software services. These controls enable AuditBoard to meet our SLA commitments around service availability, recovery time objective, recovery point objective, and security, while also enabling AuditBoard to continually enhance and develop our security and privacy programs to the benefit of all customers. This means, however, that we cannot contractually commit to individual customers' security and privacy standards or policies. In order to provide transparency, visibility and continuous assurance to our customers as to the effectiveness of our security and privacy controls, AuditBoard conducts SOC Type II audits and makes the result of these independent third-party audit reports available to our customers upon written request.

6. Why can't my privacy exhibits be attached to the contract?

Our Data Processing Addendum (DPA) details the terms and conditions applicable to AuditBoard's processing of personal data, and provides our customers with contractual protections relating to AuditBoard's compliance with data protection laws applicable to AuditBoard as a service provider and data processor. Similar to Salesforce and Workday, all customers are on the same version of the AuditBoard platform. AuditBoard provides its software on a single code line and on the same operational infrastructure, using the same privacy controls for all our customers. This means, however, that we cannot contractually commit to individual customers' DPAs or similar privacy exhibits without breaking our one-to-many business model as such privacy exhibits will likely require heavy modification to fit this one-to-many business model.

7. What types of data should customers not upload into AuditBoard?

AuditBoard is an audit enablement platform that empowers audit professionals to be more effective at their jobs. AuditBoard is designed to host its customers' audit content and collateral. However, customers must not upload protected health information, payment card information, or information relating to identified or identifiable individuals (other than users of the service). This information is not needed by AuditBoard to provide the service, nor is sharing it necessary for our customers to obtain the full benefit of the service. Additionally, AuditBoard has been built to allow customers to leverage their existing data storage (Box, Google Drive, etc.) so sensitive data stored outside of AuditBoard may still be referenced and easily accessed through URL links.

8. How do we get our data back when the relationship ends?

Customers always own their data throughout the course of the relationship. Customers can download copies of their data stored in the AuditBoard service at any time during the term. AuditBoard has a standard process for a final data download if the customer relationship ends, which can be found in the Subscription Agreement.

9. Does AuditBoard offer an SLA?

Yes, AuditBoard has a Service Level Agreement as part of the Subscription Agreement, so customers always know our commitments regarding technical support, service level obligations, and/or availability requirements. The success of AuditBoard's one-to-many cloud delivery business model is predicated upon the efficiency of our infrastructure. Since AuditBoard has the same operational business model for our entire customer base, the SLA cannot be modified on a customer by customer basis.

10. Does AuditBoard offer a termination for convenience?

AuditBoard does not offer a termination for convenience. A core element of AuditBoard's business model, and one of the ways that we provide exceptional value to our customers, is that the parties enter into at least a fixed annual term and often a multi-year agreement that both parties are committed to during the specified term. Annual and multi-year terms allow us to provide significant savings compared to a month-to-month subscription term. Customers always have the ability to terminate in the unlikely event of a material breach by AuditBoard and if this occurs, we will refund any prepaid fees covering the remainder of the term after the effective date of termination.

11. Does AuditBoard offer an acceptance test period?

Since AuditBoard runs its software for all customers on a single code line, the viability of the service has already been demonstrated by the existing customers who run their businesses on

the same single code line. Consequently, the concept of an acceptance test is made obsolete and therefore does not exist in AuditBoard's business model.

12. Will AuditBoard permit customers to audit AuditBoard?

To maintain the security of AuditBoard's service and facilities for all customers, AuditBoard does not allow customer audits. To provide customers with objective evidence that AuditBoard is maintaining its security controls, AuditBoard engages a third party to produce SOC 2 audit reports, which are available upon written request. Be sure to let us know if you have additional questions or concerns about our security environment and we will provide additional information and answer any security questionnaires.

13. Does AuditBoard offer unlimited liability for data protection?

We understand that our customers are concerned about data protection and protecting the security and privacy of our customers' data is paramount to AuditBoard. AuditBoard does not agree to unlimited liability for data protection because data security and privacy are a shared responsibility when using the software, and therefore a shared liability. AuditBoard commits to stringent, technical, and administrative security measures; however, the customer is in sole control of the type and substance of information that is uploaded to the software, and the designation and oversight of users. Ultimately, the software service is not priced to underwrite unlimited liability, and the limitation of liability must directly relate to the Subscription Agreement's terms and commercial relationship between the parties.

14. Other damages/breaches are subject to limitation of liability:

AuditBoard agrees to uncapped liability for direct damages under our intellectual property indemnity as set forth in Section 9.1 of the Subscription Agreement and for direct damages caused by gross negligence, willful misconduct, or fraud. A fundamental principle of AuditBoard's business model is that any other damages and other breaches are subject to the limitation of liability (see Section 9.1 of the Subscription Agreement).