TermTrax

Software Review Report

QuickBooks

Generated: 2026-08-09T12:58:13.058Z
Schema Version: 1.2.0

Table of Contents

Review Summary

Review ID: r13cay6ky09ld6c12i94dyp6
Status: ANALYSIS
Decision: Pending
Created At: 2026-07-14T11:31:32.678Z
Submitted At: Not submitted
Submitted By: N/A
Analysis Completed At: 2026-08-09T12:33:48.808Z
General Notes: None
Usage Conditions: None
AI Jurisdiction: California, United States (with Federal Arbitration Act overlay for dispute resolution)
Human Jurisdiction: N/A

Intake Form

Purpose: manage bookkeeping, track income and expenses, process payroll, and generate custom financial reports.
Risk Concerns: None
Review Priorities: None

Playbook Items

Name	Category	Weight	AI Color	Human Color
Audit Logging	Security Operations	HIGH	At Risk	Unaddressed
Authorized Equipment & Software	Access & Personnel	HIGH	Needs Review	Unaddressed
Termination Obligations	Termination	MEDIUM	Needs Review	Unaddressed
License Grant to Data – Our Company to Vendor	License Grant	CRITICAL	Needs Review	Unaddressed
Payment Terms	Commercial Terms	HIGH	Needs Review	Unaddressed
Data Backup & Restoration	Business Continuity	HIGH	Needs Review	Unaddressed
Data Segregation	Data Handling	HIGH	At Risk	Unaddressed
Confidentiality	Confidentiality	HIGH	At Risk	Unaddressed
Subprocessor Change Notification	Subprocessors	HIGH	At Risk	Unaddressed

Name	Category	Weight	AI Color	Human Color
Cybersecurity Prevention Systems	Security Operations	HIGH	Needs Review	Unaddressed
Disaster Recovery Testing	Business Continuity	HIGH	Needs Review	Unaddressed
Arbitration or other dispute resolution process	Legal & Compliance	MEDIUM	At Risk	Unaddressed
Subprocessor Audit Rights	Subprocessors	MEDIUM	Needs Review	Unaddressed
Cyber Risk Insurance	Governance & Risk Transfer	MEDIUM	Needs Review	Unaddressed
Assignment	Legal & Compliance	ACCEPTABLE_TO_DEVIATE	At Risk	Unaddressed
Compliance with Referenced Laws	Legal & Compliance	HIGH	Needs Review	Unaddressed
Regulatory Disclosure Procedure	Breach & Incident Response	HIGH	At Risk	Unaddressed
Encryption in Transit	Encryption	HIGH	Needs Review	Unaddressed
Subprocessor Agreements	Subprocessors	CRITICAL	Needs Review	Unaddressed
Data Processing Security Policies	Security Operations	HIGH	Aligned	Unaddressed
Processing Limitation	Data Handling	CRITICAL	Needs Review	Unaddressed
No AI/ML Training on Our Data	Data Handling	CRITICAL	At Risk	Unaddressed
Modification of Terms	Legal & Compliance	HIGH	Needs Review	Unaddressed
Breach Notification Timeline	Breach & Incident Response	CRITICAL	At Risk	Unaddressed
Our liability	Limitation of Liability	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Employee Access Control	Access & Personnel	HIGH	Needs Review	Unaddressed
Publicity	Publicity	HIGH	Needs Review	Unaddressed
Physical Security Controls	Security Operations	HIGH	Needs Review	Unaddressed
Insurance	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Data Protection Officer (DPO)	Governance & Risk Transfer	MEDIUM	Aligned	Unaddressed
Termination for Convenience	Termination	ACCEPTABLE_TO_DEVIATE	At Risk	Unaddressed
Data Ownership	Data Handling	CRITICAL	At Risk	Unaddressed
User Authentication Policies	Security Operations	HIGH	Aligned	Unaddressed
Retention of our Rights to our Property	Intellectual Property	CRITICAL	Needs Review	Unaddressed
Governing Law	Legal & Compliance	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Data Subject Rights Assistance	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Processing Location Restrictions	Data Handling	HIGH	Needs Review	Unaddressed
Employee Offboarding Access	Access & Personnel	HIGH	At Risk	Unaddressed
Vendor's liability	Limitation of Liability	HIGH	At Risk	Unaddressed
Security Training	Access & Personnel	MEDIUM	Needs Review	Unaddressed
Indemnification – Vendor to Our Company	Indemnification	MEDIUM	At Risk	Unaddressed
Vendor Audit Rights	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Non-Solicitation of Employees	Operations	MEDIUM	Aligned	Unaddressed

Name	Category	Weight	AI Color	Human Color
Anti-Virus Solution	Security Operations	HIGH	At Risk	Unaddressed
Data Retention & Deletion	Data Handling	HIGH	Needs Review	Unaddressed
Automatic Renewal	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Ownership of Custom Deliverables	Intellectual Property	HIGH	At Risk	Unaddressed
Termination for Cause	Termination	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Password Encryption	Encryption	HIGH	Needs Review	Unaddressed
Exclusivity	Operations	HIGH	Aligned	Unaddressed
Security Certifications	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Warranty & Remedy	Commercial Terms	ACCEPTABLE_TO_DEVIATE	At Risk	Unaddressed
Encryption at Rest	Encryption	HIGH	Needs Review	Unaddressed
Breach Indemnification	Governance & Risk Transfer	HIGH	At Risk	Unaddressed
Indemnification – Our Company to Vendor	Indemnification	MEDIUM	Needs Review	Unaddressed
License Grant – Vendor to Our Company	License Grant	HIGH	Needs Review	Unaddressed
Employee Confidentiality Agreements	Access & Personnel	HIGH	Needs Review	Unaddressed
Restrictions on Use	Operations	HIGH	Aligned	Unaddressed
Compliance Monitoring	Governance & Risk Transfer	HIGH	At Risk	Unaddressed

Audit Logging

AI Comment: The playbook item requires a contractual commitment to audit logging — specifically, the capability to examine whether and by whom personal data has been entered into, modified, or removed from data processing systems. No provision in any of the five provided documents (Terms of Service, Global Privacy Statement, QBO DPA, Workforce DPA, Acceptable Use Policy) specifically addresses this requirement.

The closest relevant language appears in: (1) the security measures clauses in both DPAs (QBO DPA §4.1; Workforce DPA §2.5), and (2) the audit/inspection rights provisions in both DPAs (QBO DPA §5; Workforce DPA §2.11). None of these provisions meet the audit logging standard, however:

The security measures clauses enumerate technical controls — encryption, confidentiality/integrity/availability/resilience controls, availability restoration capabilities, and security testing processes — that represent a general information security framework. None specifically commits to maintaining or making available access logs that identify who entered, modified, or deleted personal data in processing systems. These controls address security incident prevention and response; they do not address the granular PII access tracing the playbook item requires.

The audit rights provisions allow customers to: (a) review Intuit's security audit reports (e.g., SOC 2 Type II) and submit written questions about data processing (QBO DPA §5); and (b) submit written audit questions about Intuit's security practices once per year (Workforce DPA §2.11). Both provisions enable transparency about Intuit's aggregate security compliance posture — not access to per-event logs documenting individual user interactions with personal data.

Audit logging (NIST SP 800-92, SOC 2 CC7.2, ISO 27001 Annex A.12.4) is a foundational control for financial SaaS environments processing bookkeeping, payroll, and sensitive employee data. QuickBooks handles highly sensitive financial data, making the inability to determine who accessed or modified that data a material accountability gap. While Intuit's security compliance page (referenced in both DPAs) implies operation under frameworks that typically require logging, no contractual commitment to provide this capability to customers appears anywhere in the document set.

Per the Silence Handling framework: HIGH weight item !' default classification RED. No statutory downgrade applied: California CCPA does not specifically mandate contractual audit logging commitments as a standalone enforceable requirement that would substitute for this provision. No industry norm downgrade applied: for a HIGH weight item on a financial data SaaS with payroll capabilities, logging of PII access is not a low-risk gap — the sensitivity of data processed (financial records, payroll, employee PII) makes its absence a genuine and non-trivial risk that warrants the RED classification without downgrade.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.

1. "Intuit shall respond to any written audit questions related to Intuit's security practices submitted to it by Customer, provided that Customer shall not exercise this right more than once per year."

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
>
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

> *"Section 5 (Security Reports and Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense)."*
>
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
>
> — QuickBooks Time & Workforce (Time/Payroll) DPA

Authorized Equipment & Software

AI Comment: The playbook item imposes two specific, endpoint-level security controls: (1) vendor employees must process customer data exclusively on authorized business equipment; and (2) the vendor must prevent the use or installation of unauthorized hardware and software on systems that process customer data. Neither requirement is expressly addressed in any of the reviewed documents.

Both DPAs (the QB Online DPA, Doc 3, and the QB Workforce/Time DPA, Doc 4) commit Intuit to implementing "appropriate technical and organizational measures" to protect customer data — a standard GDPR-derived obligation — with a non-exhaustive enumerated list covering encryption/pseudonymization, system confidentiality and resilience, incident recovery capability, and periodic testing of security effectiveness. The DPAs also impose confidentiality obligations on all personnel authorized to process customer data. These provisions address the 'who' (authorized persons) and the general security framework, but they do not address the 'what hardware/software' question. Neither DPA's illustrative list of TOMs includes authorized-equipment-only policies, endpoint device management, or controls blocking unauthorized software installation.

The QB Online DPA (§ 5) makes security audit reports available to the customer, which in practice could surface Intuit's actual endpoint controls (e.g., a SOC 2 Type II report commonly covers endpoint protection). However, making audit reports available for review is not a contractual commitment to the specific controls the playbook requires and cannot substitute for an express contractual obligation.

Because the documents address security in general — but leave the specific authorized-equipment and unauthorized-software-prevention requirements unaddressed — this item is classified YELLOW rather than RED. For a High weight item, this gap warrants documented assessment. The reviewing team should consider requesting a security exhibit, a completed security questionnaire, or a SOC 2 report excerpt that explicitly confirms authorized-equipment-only processing environments and endpoint software controls are operative for all systems handling customer data.

— Superseding reasoning —
The QB Online DPA (Doc 3, § 11.3) explicitly establishes its own precedence over the Agreement (ToS) for matters within its scope: SCCs prevail first, then the DPA, then the Agreement. Accordingly, the DPA security provisions (§§ 4.1–4.2) govern over any general security statements in the ToS for Business Connection Data processed under the QB Online service. The QB Workforce/Time DPA (Doc 4) similarly controls over the Agreement for discrepancies relating to Customer Data processed under Time, Workforce, and Contractor Payments services. No conflict exists between the two DPAs on this specific item because they operate on parallel, non-overlapping service scopes (QB Online vs. QB Workforce/Time); neither supersedes the other. Both DPAs converge on the same conclusion: general TOMs commitment without specific authorized-equipment or unauthorized-software-prevention language.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"
2. "Intuit shall ensure that any person that it authorizes to Process the Customer Data (including Intuit's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of …"

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of*

implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymisation or encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."
— QuickBooks Time & Workforce (Time/Payroll) DPA

Termination Obligations

AI Comment: The playbook item requires that upon termination the Vendor must return or make available all of the customer's data. The document set addresses this obligation across multiple instruments, but collectively falls short of the "all data" standard due to scope limitations and significant carve-outs.

ToS (Document 1): The base Terms of Service contain no affirmative data-return obligation at termination. The only reference is a self-service instruction for users to delete data through account settings (Section A, Termination). This is superseded by the DPAs per their explicit hierarchy clauses and is not the governing position.

QBO DPA (Document 3, Section 7) — governing for QBO data: Upon termination, Intuit must "take reasonable measures to provide tools for Customer (at Customer's election) to delete or return to Customer all Business Connection Data." Three limitations prevent full compliance with the playbook item: (1) Scope — coverage is expressly limited to "Business Connection Data," defined as personal data of the customer's customers, vendors, employees, and prospects. Core non-personal financial data (e.g., chart-of-accounts structures, aggregated ledger entries, financial reports) may fall outside this definition and carry no contractual return obligation. (2) Mechanism — Intuit provides tools for the customer to self-effectuate the return, rather than proactively returning data. (3) Backup carve-out — data archived in backup systems is explicitly excluded from the return obligation; Intuit need only isolate and eventually delete it. An additional controller-role carve-out (also Section 7) means data Intuit continues to process as a data controller need not be returned at all.

Time & Workforce DPA (Document 4, Section 2.10) — governing for Time/Workforce/Contractor Payments data: This instrument is marginally more favorable. At the customer's election, Intuit must return or destroy all Customer Data (not merely provide tools). The customer can affirmatively elect "return," giving a stronger right. However, backup data is again excluded, and "Customer Data" for these services may be narrower than the customer's full data universe in QuickBooks.

Overall: The topic is meaningfully addressed, but the acceptable position ("return or make available all of our data") is not satisfied in full. The scope gap (non-personal financial data), the backup carve-out, and the controller-role exclusion each contribute to material residual risk. Classification is YELLOW at Medium weight — moderate risk, requiring documented justification.

— Superseding reasoning —
The QBO DPA (Document 3, Section 11.3) establishes an explicit document hierarchy: SCCs prevail first, then the DPA, then the Agreement (Terms of Service). Accordingly, DPA Section 7's data return provisions supersede the ToS's more limited self-service data deletion instructions for Business Connection Data. Similarly, the QuickBooks Time & Workforce DPA (Document 4) states that "In the event of any discrepancies between the terms of this DPA and the Agreement with respect to the Processing of Customer Data, this DPA shall control." Both DPAs therefore govern data return upon termination for their respective service categories, displacing the ToS termination provisions on this topic.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "At Customer's election, Intuit shall return or destroy all Customer Data in its possession or control (including in the possession of any Subprocessor) in accordance with Intuit's data retention and d…"
*"Termination**"*
— QBO Terms of Service for QuickBooks - US
"Section 7 (Return or Deletion of Data) of this DPA."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Further, the parties acknowledge and agree that Intuit shall not be required to delete or return Business Connection Data which it continues to process for the limited controller purposes described in this DPA and the relevant Agreement

(and in accordance with Intuit's internal retention criteria)."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

License Grant to Data – Our Company to Vendor

AI Comment: The acceptable position requires the vendor license to be non-exclusive. That minimum standard is satisfied: the Section A content license is explicitly designated "Non-exclusive, which means you can license your Content to others" (PIF [0]), and the Workforce-specific Section B license is also explicitly "non-exclusive" (PIF [3]). The QBO DPA (Document 3) adds protection by purpose-limiting Business Connection Data processing in Intuit's processor capacity and supersedes the TOS Agreement for that data category per DPA § 11.3. Classification is YELLOW — not RED — because the non-exclusive minimum is met. Classification does not reach GREEN because the license grant as a whole deviates materially from the ideal preference across all three preference dimensions:

(1) NOT REVOCABLE: The Section A license "lasts for as long as your Content is protected by intellectual property rights" — effectively perpetual. The Survival clause in Section A explicitly preserves the entire "Content and Data" section after contract termination, meaning Intuit retains its license to customer Content even after the subscription ends. No revocation mechanism is provided. The customer cannot terminate the content license upon ending the service relationship.

(2) SCOPE EXTENDS BEYOND PROVIDING THE SERVICE: The Section A license purpose extends to "improving the Platform" and "creating new features and functionalities" — Intuit's own product development activities that are not necessary to delivering QuickBooks to the customer. Additionally, the Section A Rights section expressly grants Intuit the right to "sublicense" customer Content to third parties, enabling downstream data rights that extend beyond the direct vendor relationship. The Workforce-specific license (PIF [3]) is scoped to "Intuit's lawful business purposes" — materially broader than just "providing the service" — and explicitly includes improving "other Intuit products," meaning customer payroll and employee data serves Intuit's own product portfolio beyond the contracted service.

(3) DATA USED FOR VENDOR'S OWN COMMERCIAL PURPOSES: Two provisions are especially concerning for this Critical-weight item. First, Section A's deidentified data clause (PIF [2]) goes beyond a license — Intuit claims OWNERSHIP of deidentified and aggregated data derived from customer Content, with authorization to use it "without restriction," including "marketing Intuit's products and services." Marketing Intuit's own services is an unambiguous commercial own-purpose use. Second, DPA § 2.1 (PIF [4]) explicitly carves out Intuit's right to act as a data controller for Business Connection Data for "product development and improvement, data analytics...and to market Intuit's products and services" — again, Intuit's own commercial interests, not the customer's contracted service.

The DPA § 2.2 purpose limitation (PIF [5]) provides meaningful protection for Business Connection Data in Intuit's processor role and supersedes the TOS for that data category per DPA § 11.3. However, it does not extend to: (i) Intuit's controller activities, which are governed by § 2.1 and explicitly authorize marketing and product development use (PIF [4]); or (ii) deidentified data, which falls outside DPA scope as no longer personal data and is instead governed by the unrestricted Section A ownership clause (PIF [2]). For a Critical-weight item involving highly sensitive financial data — bookkeeping, payroll, income/expense records, and financial reporting per the intake brief — the combined effect of the non-revocable scope, improvement-purpose extension, sublicensing rights, deidentified data ownership for marketing, and the DPA controller marketing carve-out represents materially weaker protection than the ideal preference contemplates and warrants close legal review before acceptance.

— Superseding reasoning —
Three superseding relationships apply. First, DPA § 11.3 establishes an explicit order of precedence: "the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement." Accordingly, DPA § 2.2's processor-capacity purpose limitation (PIF [5]) supersedes the TOS Section A content license scope (PIF [0]) and the TOS content license rights/purpose provision (PIF [1]) for Business Connection Data processed in Intuit's processor capacity. Second, within the TOS itself, the Section B introduction states: "These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms." The Workforce-specific license in Section B, Part F § 15 (PIF [3]) therefore supersedes the Section A general content license (PIF [0]) for Workforce Services Personal Information. Third, note that DPA §§ 2.1 and 2.2 do not supersede each other — they operate in parallel for different processing roles. Section 2.1 (controller activities for product development and marketing) and Section 2.2 (processor activities per customer instructions) coexist; the controller carve-out in § 2.1 limits the scope of the § 2.2 purpose limitation for certain data uses but does not supersede it. Finally, the deidentified data ownership provision (PIF [2]) is not superseded by the DPA: the DPA governs "Business Connection Data" (personal data), while deidentified/aggregated data is, by definition, no longer personal data and falls entirely outside DPA scope.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "This license allows Intuit to: Host, reproduce, distribute, communicate, sublicense and use your Content — for example, to save your Content on our systems and make it accessible from anywhere you go;…"
2. "Intuit may collect, derive or generate deidentified and/or aggregated data regarding your usage of or the performance of the Platform, including data derived from your Content. Intuit will own all suc…"
3. "In your use of the Workforce Services you are hereby granting Intuit a non-exclusive, worldwide, royalty-free right and license to collect, use, copy, display, perform, store, transmit, modify and cre…"
4. "Intuit shall process Business Connection Data, as further described in Annex A (Details of Data Processing) of this DPA, only in accordance with Customer's documented lawful instructions as set forth …"

"Non-exclusive, which means you can license your Content to others"
— QBO Terms of Service for QuickBooks - US

> *"Provided, however, that the parties acknowledge that Intuit shall be a controller when Intuit uses Business Connection Data for certain limited purposes, as further described in the Agreement (including, for example, in relation to Intuit product development and improvement, data analytics, and fraud prevention and security), for product and service improvement, and to market Intuit's products and services."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Payment Terms

AI Comment: The QuickBooks Online Terms of Service establish an automatic/prepay billing model rather than a traditional invoice-based arrangement with a 30-day payment window. The acceptable position has two pathways: (a) NET 30 from invoice receipt, or (b) credit card autopay.

Pathway (a) – NET 30 invoice terms: Not present. The Terms charge "upon purchase and when you provide your payment information" (Section A, Payment & Cancellations), and subscription fees are billed in advance. No provision offers a 30-day post-invoice payment grace period.

Pathway (b) – Credit card autopay: Partially met. Intuit's model is fundamentally autopay — charges are made automatically to the configured payment method and subscriptions auto-renew. If the customer configures a credit card as the payment method, the arrangement is credit card autopay, satisfying the exception. However, Intuit equally permits bank account/ACH payment for these automated charges. Because the Terms do not restrict payment to credit card only, strict alignment with "credit card autopay" depends entirely on which payment method the customer elects — a fact not fixed in the contract itself.

Additional context: For annual subscriptions, Intuit provides 30–60 days' advance notice before the renewal charge (§ Payment & Cancellations, sentence 1-54). This is a renewal reminder, not an invoice with a payment window, and does not satisfy the NET 30 requirement. For Bill Pay fees specifically, the Terms use the word "invoiced," but charges are executed automatically at the start or end of the billing cycle — no actionable payment window from the invoice date.

Classification rationale: YELLOW because (1) no traditional NET 30 invoice-based terms exist anywhere in the document set; (2) the autopay model is present and aligns with the spirit and possibly the letter of the credit card autopay exception; but (3) the "credit card" specificity is not contractually locked — bank/ACH is an equal option — meaning compliance with the exception depends on a customer configuration choice rather than a contractual commitment. The risk is low in practice (SaaS autopay billing is predictable and standard), but the legal team should confirm the company configures credit card as its payment method to definitively satisfy the playbook exception. High-weight item warrants documentation of that configuration decision.

> *"Payments will be billed in U.S. dollars, and your account will be charged upon purchase and when you provide your payment information, unless stated otherwise in applicable payment provisions."*
> — QBO Terms of Service for QuickBooks - US
> *"You may be charged a subscription fee in advance on an annual basis or other recurring interval disclosed to you prior to your purchase."*
> — QBO Terms of Service for QuickBooks - US
> *"For annual subscriptions, we will send you a reminder with the then-current subscription fee no less than thirty (30) days and no more than sixty (60) days before your subscription term ends, or otherwise as required by applicable law."*
> — QBO Terms of Service for QuickBooks - US
> *"Your payment to Intuit will automatically renew at the end of the applicable subscription period but you can cancel a subscription at any time."*
> — QBO Terms of Service for QuickBooks - US
> *"You will be invoiced for Bill Pay Fees along with other amounts that you owe as a QuickBooks Online customer. All subscription fees will be charged at the beginning of your billing cycle and all transaction fees will be charged at the end of your billing cycle."*
> — QBO Terms of Service for QuickBooks - US

Data Backup & Restoration

AI Comment: The playbook item requires two specific, affirmative commitments: (1) the vendor shall create backups of customer data, and (2) the vendor shall regularly conduct restoration tests of those backups at a minimum annual frequency. The documents partially address these requirements but fall meaningfully short of both specifics.

Primary Governing Source — QBO DPA Section 4.1: The most substantive relevant language appears in the QuickBooks Online DPA Section 4.1 Security Measures, which adopts GDPR Article 32–style enumeration and commits Intuit to measures "as appropriate" including: "(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; [and] (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." This language implicitly encompasses backup infrastructure (restoration ability presupposes data copies) and implies periodic testing of technical controls. However, it stops well short of the playbook's requirements because: (a) it frames restoration as a *capability* ("the ability to restore") rather than an explicit commitment to *create and maintain* backups; (b) sub-item (d)'s testing obligation is general across all technical/organizational measures, not specific to backup restoration tests; and (c) no minimum frequency (annual or otherwise) is specified for restoration testing.

Backup Existence Corroborated — DPA Section 7 and QB Time DPA Section 2.10: Both the QBO DPA Section 7 and the QuickBooks Time/Workforce DPA Section 2.10 make incidental reference to "back-up systems" in the context of data deletion upon termination (carving out backup copies from deletion obligations due to cost and technical difficulty). This corroborates that Intuit maintains backup infrastructure, but these references arise in the context of deletion mechanics, not as affirmative commitments to create or maintain backups for data recovery purposes. They do not address restoration

testing at all.

ToS Disclaimer — Superseded: The Terms of Service Disclaimers section explicitly disclaim warranties "with respect to data loss," which on its face would undercut any expectation of backup adequacy. However, per QBO DPA Section 11.3's explicit precedence hierarchy (SCCs > DPA > Agreement), the DPA's affirmative security commitments in Section 4.1 govern over the ToS disclaimer for data processing matters. The operative language is therefore DPA Section 4.1, not the ToS disclaimer.

QB Time/Workforce DPA Section 2.5: For Workforce and Time services specifically, Intuit commits to "appropriate technical and organizational measures" but without enumeration of the specific sub-items (restoration capability, regular testing) that appear in the QBO DPA Section 4.1. This is a weaker formulation for those services.

Net Classification — YELLOW: The contract addresses data resilience through general security measure commitments that include restoration capability and periodic testing of technical controls, meaning the topic is not wholly silent. But the contract falls short of the acceptable position on both prongs: there is no explicit commitment to *create* backups, and there is no explicit commitment to conduct restoration *tests* with a minimum annual frequency. The gap is in specificity and precision rather than complete absence. For a HIGH weight item, this ambiguity carries meaningful risk — particularly for a SaaS solution processing bookkeeping, payroll, and financial report data where backup integrity is operationally critical.

— Superseding reasoning —
The Terms of Service Disclaimers section (ToS, PIF index 2) disclaim warranties for data loss, which conflicts with the DPA Section 4.1 (PIF index 0) affirmative restoration and testing commitments. Per QBO DPA Section 11.3's explicit precedence hierarchy — "(i) SCCs; then (ii) this DPA; and then (iii) the Agreement" — the DPA governs over the Agreement (ToS) in matters of data processing. Accordingly, DPA Section 4.1's restoration capability and regular testing commitments supersede the ToS data-loss disclaimer for purposes of this playbook item's analysis.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Upon termination or expiration of the Agreement, Intuit shall take reasonable measures to provide tools for Customer (at Customer's election) to delete or return to Customer all Business Connection Da…"
2. "This requirement shall not apply: (a) to the extent that Intuit is required by any Applicable Data Protection Law to retain some or all of the Customer Data, in which event Intuit shall isolate and pr…"

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"We also do not provide any warranties with respect to data loss or to the accuracy, reliability, or availability of the Platform, nor of any content (including any Content) or information made available in the Platform."*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA

Data Segregation

AI Comment: The playbook item requires physical and/or logical separation of data received from different controllers. No document in the set contains an explicit commitment to physical or logical data segregation between controllers. The finding is RED for this High weight item for three compounding reasons:

1. Active cross-platform data integration language cuts directly against segregation. The ToS instructs that by using the platform users are directing Intuit to share their data "across our Platform for marketing, eligibility, and other purposes." The Global Privacy Statement doubles down, stating Intuit "uses that data together to power experiences across the Intuit Platform and products, not just within the individual offering(s) you're using." This is affirmative, operational language describing the absence of controller-to-controller data segregation in platform architecture.

2. Controller-mode carve-outs allow cross-platform data use even for Business Connection Data. QBO DPA §2.1 explicitly acknowledges that Intuit acts as an independent data controller—not a processor—when it uses Business Connection Data for "product development and improvement, data analytics, and fraud prevention and security." In that

controller mode, the Global Privacy Statement governs, and the platform-wide integration approach applies. There is no segregation requirement covering Intuit's controller-capacity processing.

3. The closest functional approximation—CCPA non-combination clauses—falls materially short of the playbook requirement. Both DPAs (QBO DPA Annex B, item 11; QB Workforce DPA §3.1) prohibit combining Business Connection Data from one customer with data from other customers or third parties, except for Permitted Purposes. This logically implies some separation of outputs but is insufficient: (a) it applies only in the CCPA/Service Provider context and contains a Permitted Purpose exception; (b) it addresses data combination at the use/disclosure layer, not physical or logical segregation of storage and processing environments; (c) it does not apply when Intuit processes Business Connection Data in its controller capacity (DPA §2.1). The QBO DPA §2.2 purpose limitation and security measures (§4.1: encryption, pseudonymization) similarly address adjacent concerns but do not constitute commitments to controller-to-controller segregation architecture.

Superseding note: The QBO DPA §11.3 establishes DPA > Agreement in order of precedence. The DPA's purpose limitation clause (§2.2) accordingly supersedes the ToS general cross-platform data sharing instruction for Business Connection Data in Intuit's processor role. However, DPA §2.1's explicit controller carve-out means the ToS/Privacy Statement integration approach continues to govern when Intuit acts as controller for analytics and product improvement—limiting the practical effect of that superseding determination. No document at any level of the hierarchy provides an explicit physical/logical segregation commitment.

— Superseding reasoning —
QBO DPA §11.3 establishes a clear precedence order: SCCs, then DPA, then the Agreement (ToS). For Business Connection Data processed in Intuit's capacity as processor, the DPA §2.2 purpose limitation (restricting processing to documented lawful instructions) is more specific and hierarchically superior to the ToS's general cross-platform data sharing instruction, and therefore supersedes it. However, DPA §2.1 expressly preserves Intuit's controller role for certain processing activities (product development, analytics, fraud prevention), meaning the ToS/Privacy Statement cross-platform integration approach continues to govern that subset of processing. The superseding effect is therefore partial rather than absolute.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall process Business Connection Data, as further described in Annex A (Details of Data Processing) of this DPA, only in accordance with Customer's documented lawful instructions as set forth …"
2. "At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall include, as appropriate: (a) th…"
3. "Without limiting the data use rights set forth herein, as a Service Provider, Intuit will not: sell or share any Business Connection Data; retain, use, or disclose any Business Connection Data (i) for…"
4. "Intuit will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Agreement, …"

> *"Agreement to These Terms"*
> — QBO Terms of Service for QuickBooks - US
> *"The Intuit platform"*
> — Global Privacy Statement | Intuit
> *"the parties acknowledge that Intuit shall be a controller when Intuit uses Business Connection Data for certain limited purposes, as further described in the Agreement (including, for example, in relation to Intuit product development and improvement, data analytics, and fraud prevention and security)"*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Confidentiality

AI Comment: The playbook item's acceptable position requires: (1) that Intuit not disclose the organization's Confidential Information to third parties except on a need-to-know basis to perform the services, (2) standard carve-outs (previously known, independently developed, rightfully received from a third party, in the public domain), and (3) ideally, mutual confidentiality obligations. None of these three requirements are fully met.

ABSENCE OF A GENERAL CONFIDENTIALITY CLAUSE: No document in the set — the ToS, either DPA, the Privacy Statement, the Telecom Terms, or the AUP — contains a traditional confidentiality clause that protects "Confidential Information" as a defined category. The term "Confidential Information" does not appear at all in the conventional NDA sense. This is characteristic of a click-wrap SaaS ToS that is not designed to be supplemented by a mutual NDA at the point of acceptance.

WHAT THE DOCUMENTS DO PROVIDE — NARROW DATA-PROCESSING CONFIDENTIALITY: Both the QBO DPA (§4.2, §3.2) and the Time/Workforce DPA (§2.4, §2.6) contain "confidentiality of processing" provisions. These require that Intuit's authorized persons and subprocessors maintain confidentiality obligations with respect to "Business Connection Data" (QBO DPA) or "Customer Data" (Time/Workforce DPA) — both defined to mean personal data of customers, employees, vendors, and prospects. These provisions partially address the need-to-know element of the acceptable position, but only for this narrow subset of information. The protection explicitly does not extend to the organization's broader Confidential Information — e.g., proprietary financial models, business plans, trade secrets, or operational methodologies that do not constitute "personal data" as defined. Both DPAs prevail over the ToS by explicit precedence clause for their respective data categories; accordingly, for personal data, the DPA confidentiality provisions displace the ToS content license. However, the ToS governs all other customer content without restriction.

ACTIVE CONTRADICTION — ToS CONTENT LICENSE: The ToS grants Intuit a worldwide, royalty-free license expressly including sublicensing rights over all customer content, for the purpose of operating, providing, and improving the Platform. The sublicensing right enables Intuit to share customer content with third parties. For non-personal customer content (which may include highly sensitive business records), no confidentiality obligation constrains this sublicensing. Separately, the ToS grants Intuit ownership of, and unrestricted rights to use, any deidentified or aggregated data derived from customer content — including for marketing purposes. Both rights are confirmed by, or consistent with, the DPAs (the QBO DPA Annex B expressly permits Intuit to de-identify Business Connection Data), meaning the DPAs do not cure these provisions.

STANDARD CARVE-OUTS: The standard carve-outs required by the acceptable position (previously known, independently developed, rightfully received from a third party, in the public domain) are not defined or referenced in any confidentiality context across any document in the set. California law provides limited common-law protections, but the absence of contractually defined carve-outs leaves the scope of any confidentiality obligation (to the extent one exists) undefined and unenforceable as contemplated.

MUTUAL CONFIDENTIALITY: No mutual confidentiality obligations exist. The arrangements are entirely one-directional: the DPAs impose data processing constraints on Intuit with respect to customer personal data, but the organization has no corresponding obligations to protect Intuit's information, and more importantly, Intuit makes no general commitment to protect the organization's Confidential Information outside of personal data processing contexts.

NET ASSESSMENT: The DPA provisions provide meaningful but narrowly scoped protection for personal data (YELLOW on that dimension). However, because the acceptable position requires confidentiality protection for Confidential Information broadly — not just personal data — and because (a) the ToS content license actively enables disclosure of non-personal customer content to third parties, (b) standard carve-outs are entirely absent, and (c) this is a High-weight item, the overall classification is RED. The preference for mutual confidentiality is also unmet.

— Superseding reasoning —
The QBO DPA (§11.3) and Time/Workforce DPA ("How this DPA applies") each contain explicit precedence clauses: the QBO DPA states it prevails over the Agreement in the following order — (i) SCCs, then (ii) DPA, then (iii) Agreement (ToS); the Time/Workforce DPA states it controls over the Agreement for discrepancies regarding Processing of Customer Data. Accordingly, for Business Connection Data (QBO DPA) and Customer Data (Time/Workforce DPA), the DPA confidentiality of processing provisions supersede the ToS content license to the extent they conflict. The superseding relationship is grounded in document hierarchy (explicit contractual priority) and specificity (DPAs are specific data-processing instruments; ToS is a general platform agreement). The ToS content license and deidentified data rights, however, continue to govern customer content that does not constitute Business Connection Data or Customer Data — the DPAs do not eliminate those ToS provisions for non-personal content. The net effect is that the DPA confidentiality provisions govern a narrowly defined subset of the organization's information (personal data), while the ToS governs everything else without confidentiality constraint.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "This license allows Intuit to:

Host, reproduce, distribute, communicate, sublicense and use your Content — for example, to save your Content on our systems and make it accessible from anywhere you go…"
2. "Intuit shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Business Connection Data as those…"
3. "Intuit shall ensure that any person that it authorizes to Process the Customer Data (including Intuit's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of …"

> *"Content and Data"*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Intuit imposes data protection terms on any Subprocessor it appoints that are consistent with the terms of this DPA; and*
>
> *Intuit remains fully liable for any breach of this Clause that is caused by an act, error or omission of its Subprocessor that is acting on our behalf under this DPA."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA

Subprocessor Change Notification

AI Comment: The playbook's acceptable position requires three things: (1) notification of any new or replacement subprocessor, (2) at least 30 days from notice within which the customer may object, and (3) a right to terminate with a pro-rata refund of unused fees if the vendor proceeds despite the customer's objection. The ideal preference adds a fourth requirement: advance notice delivered before the subprocessor begins processing.

Two separate DPAs address subprocessor notification across the QuickBooks product suite. The QBO DPA (Document 3, §3.2) governs QuickBooks Online and related services; the QB Time & Workforce DPA (Document 4, §2.6) governs QB Time, Workforce, and Contractor Payments and expressly controls over the QBO DPA for those specific services where there is any discrepancy (QB Time/Workforce DPA §4.7).

Requirement 1 — Notification: Both DPAs provide some form of subprocessor change notification. The QB Time/Workforce DPA requires Intuit to provide "notice of the addition or removal of any Subprocessor (including details of the Processing it performs or will perform)," delivered by "posting details of such addition or removal which can be found in your Time account under 'Profile'." The QBO DPA requires Intuit to maintain and provide updated sub-processor lists. Notification is therefore present in form, but is passive (customer must check an account page) rather than proactive advance notification. This does not meet the acceptable position, which contemplates active notice to the customer.

Requirement 2 — 30-day advance notice / objection window: Neither DPA specifies a 30-day advance notice period before a new subprocessor begins processing. The QBO DPA references compliance with "Clause 9 of the 2021 Controller-to-Processor Clauses," but the document does not set out a defined advance-notice period within the DPA text itself, and the QB Time/Workforce DPA's Attachment 1 selects SCC "Option 2 in Clause 9(a)" with the "specified time period" referring back to "the notification time period set forth in the DPA" — yet no specific advance-notice period is stated anywhere in that DPA. There is no explicit 30-day (or any) window within which the customer may formally object before a new subprocessor commences processing. This requirement is entirely unmet.

Requirement 3 — Termination with pro-rata refund: The QB Time/Workforce DPA §2.6 does include a termination right: "If Customer refuses to consent to Intuit's appointment of a third-party Subprocessor relating to the protection of the Customer Data, Customer may elect to suspend or terminate the Agreement, including this DPA, subject to all fees and payment due for services rendered." However, this formulation is materially weaker than the acceptable position in two respects. First, the right is framed as upfront refusal of consent, not a post-notice objection right within a defined window. Second, and critically, termination is conditioned on the customer remaining liable for "all fees and payment due for services rendered" — there is no pro-rata refund of prepaid/unused fees. The QBO DPA has no analogous termination right for this scenario at all. Both outcomes contradict the acceptable position.

Ideal Preference: The preference — advance notice delivered before the subprocessor begins processing — is not met by either DPA. Notification via account-page posting is reactive and does not guarantee the customer will be informed before a subprocessor commences data processing.

In summary, the vendor documents partially address subprocessor notification but fail on every key protective element: no defined advance-notice period, no formal 30-day objection window, and no pro-rata refund right upon termination triggered by a subprocessor objection. For a High-weight item, this represents a material gap from the acceptable position. Classification: RED.

— Superseding reasoning —
The QB Time & Workforce DPA (Document 4) expressly states that "In the event of any discrepancies between the terms of this DPA and the Agreement with respect to the Processing of Customer Data, this DPA shall control" (§4.7). The QBO DPA (Document 3) is incorporated into the "Agreement" as defined in that instrument. For QB Time, Workforce, and Contractor Payments services, the QB Time/Workforce DPA §2.6 therefore supersedes the QBO DPA §3.2's subprocessor notification and list-maintenance provisions for those services (SPECIFIC_OVER_GENERAL / NARROW_SCOPE). The QBO DPA §3.2 continues to govern subprocessor notification for core QuickBooks Online services. Both provisions independently fail the acceptable position, so the superseding determination does not change the overall RED classification.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Business Connection Data as those…"
2. "Customer consents to Intuit engaging third-party Subprocessors to Process the Customer Data provided that:

Intuit provides notice of the addition or removal of any Subprocessor (including details of …"

Cybersecurity Prevention Systems

AI Comment: The playbook item requires the vendor to have adequate systems and processes to prevent unauthorized access to, disclosure of, or loss of customer data. This is a HIGH weight item and the document set addresses it across multiple instruments, with the QuickBooks Online Data Processing Agreement (DPA, Document 3) providing the most substantive commitments.

What the documents provide:
The DPA (Section 4.1) commits Intuit to implement "appropriate technical and organisational measures to protect Business Connection Data from a Security Incident," and enumerates specific measures consistent with GDPR Article 32: pseudonymization/encryption, ongoing confidentiality/integrity/availability/resilience, restoration capability, and a process for regular testing and evaluation. The DPA also imposes confidentiality obligations on all authorized processors (Section 4.2), a security incident notification and remediation regime (Section 4.4), and access to security audit reports and written question submission (Section 5). The Time and Workforce DPA (Document 4, Section 2.5) mirrors these commitments for payroll and workforce data. The Global Privacy Statement (Document 2) further references "reasonable physical, technical and organizational safeguards."

Why YELLOW rather than GREEN:
Despite the DPA's substantive commitments, several factors prevent a GREEN classification against the "adequate systems and processes" standard:

1. **General language without specific standards:** The security commitments use "appropriate" measures language — consistent with legal baselines (GDPR Art. 32) — but do not contractually commit to specific technical certifications (e.g., SOC 2 Type II, ISO 27001) or encryption standards. Intuit retains significant unilateral discretion in determining what is "appropriate."

2. **Residual ToS platform disclaimer:** The ToS (Section A, Disclaimers) explicitly states: "We do not warrant that the Platform is error-free, secure, or free from any viruses or other harmful components" and further disclaims warranties regarding "data loss." While the DPA supersedes the ToS for Business Connection Data processing matters (DPA Section 11.3), the ToS disclaimer continues to apply at the platform level — e.g., platform availability and system integrity outside the specific data processing scope defined in the DPA. This scope boundary creates meaningful residual ambiguity.

3. **Mutable security measures:** Section 4.3 of the DPA explicitly acknowledges that "Intuit may update or modify the Security Measures from time to time," with only a commitment against "degradation of the overall security." There is no change notification obligation to the customer when measures are altered.

4. **Limited audit rights:** Customer's ability to verify compliance is restricted to reviewing posted security audit reports and submitting written questions (once per year under the Workforce DPA). There is no right to conduct independent audits or on-site inspections.

5. **Privacy Statement qualification:** The Global Privacy Statement (the instrument governing Intuit's role as data controller) explicitly states it "cannot completely ensure or warrant the security" of personal information, undermining the strength of the underlying commitment.

Document hierarchy applied: Per DPA Section 11.3 (SCCs > DPA > Agreement), the DPA security commitments govern over the ToS Disclaimers for Business Connection Data processing. This prevents a RED finding but does not fully cure the gaps that preclude GREEN. The governing language for security of customer data in the data processing context is DPA Section 4.1. The ToS platform-level disclaimer continues to govern for matters outside the DPA's explicit scope.

— Superseding reasoning —
DPA Section 11.3 establishes explicit document hierarchy: "In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement." The DPA's affirmative security commitments (Section 4.1) therefore supersede the ToS Disclaimers section's explicit disclaimer that the Platform is not warranted to be secure and that Intuit provides no warranties regarding data loss, but only as to Business Connection Data processing matters. The ToS platform security disclaimer continues to govern for matters at the platform level that fall outside the DPA's defined scope (Business Connection Data processing), creating a residual scope ambiguity that supports the YELLOW classification. The Section B ToS terms also contain a hierarchical rule (Section B Terms prevail over Section A conflicts), but the DPA sits above both in precedence per its own terms.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer is responsible for reviewing the information made available by Intuit relating to data security and making an independent determination as to whether the Service meets Customer's requirements…"
2. "If Intuit becomes aware of an actual Security Incident that involves Business Connection Data, Intuit will: (a) notify Customer of the Security Incident without undue delay; (b) take appropriate steps…"
3. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"

> *"We do not warrant that the Platform is error-free, secure, or free from any viruses or other harmful components. We also do not provide any warranties with respect to data loss or to the accuracy, reliability, or availability of the Platform, nor of any content (including any Content) or information made available in the Platform."*
> — QBO Terms of Service for QuickBooks - US
>
> *"We will use appropriate technical and organizational measures to secure this data consistent with applicable data privacy and protection laws or regulations."*
> — QBO Terms of Service for QuickBooks - US
>
> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

> *"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."*
> — Global Privacy Statement | Intuit
> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA

Disaster Recovery Testing

AI Comment: The playbook item requires three distinct, affirmative commitments: (1) the existence of a disaster recovery (DR) plan, (2) the existence of a business continuity (BC) plan, and (3) annual testing of those specific plans. No document in the provided set explicitly commits to any of these three elements.

The closest relevant language appears in the QBO DPA (Document 3), Section 4.1 (Security Measures), which incorporates boilerplate GDPR-aligned security obligations: specifically, sub-clause (c) — the ability to restore availability and access to personal data in a timely manner following a physical or technical incident — and sub-clause (d) — a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing. These provisions address the conceptual domain of resilience and operational testing, but they are not functionally equivalent to the playbook's acceptable position because: (a) they are framed as data security obligations rather than operational DR/BC commitments; (b) they contain no explicit reference to disaster recovery plans or business continuity plans as distinct, documented frameworks; and (c) the testing requirement in sub-clause (d) specifies no frequency — "regularly" is undefined and carries no contractual floor of annual testing.

The ToS (Document 1) contains provisions that work against favorable DR commitments — Intuit reserves the right to modify, suspend, or discontinue the Platform at any time (Section "Changes") and expressly disclaims liability for such actions. Warranties for availability are also disclaimed ("we do not provide any warranties with respect to data loss or to the accuracy, reliability, or availability of the Platform").

The DPA's precedence clause (Section 11.3, Document 3) establishes that in case of conflict, the DPA governs over the ToS, so the security measure commitments in Section 4.1 would take precedence over the ToS availability disclaimers. However, even giving the DPA security language its maximum weight, it does not constitute an explicit DR/BC plan commitment or a binding annual testing obligation.

Both DPAs (Documents 3 and 4) reference external security documentation (Intuit Security Center at security.intuit.com and security.intuit.com/security-practices respectively), which may contain more detailed DR/BC commitments. However, what is actually incorporated into the contractual documents is insufficient to meet the acceptable position. Relying on non-contractual, externally-hosted security documentation that Intuit may update or retract at will does not constitute a binding contractual commitment.

Classification: YELLOW — the contract addresses related resilience and testing concepts (sub-clauses (c) and (d) of the DPA security measures), but the protection is materially weaker and narrower than the playbook's acceptable position. An explicit DR/BC plan commitment, documented and with an annual testing obligation, is absent from all provided documents. For a HIGH weight item, this warrants a documented assessment and should be escalated for legal review prior to contract execution. Reviewers should consider requesting Intuit's current DR/BC documentation and a contractual addendum confirming annual testing obligations.

— Superseding reasoning —
The QBO DPA (Document 3) Section 11.3 establishes a precedence hierarchy: SCCs prevail first, then the DPA, then the Agreement (ToS). This means the DPA security measure provisions in Section 4.1 govern over any conflicting ToS language (e.g., the broad suspension rights and availability disclaimers in Document 1). The DPA security provisions are the operative, governing language for purposes of this analysis.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "For more information about our technical and organisational measures to protect Business Connection Data from a Security Incident please visit Intuit Security Center."

> *"Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

For more information about our technical and organizational measures to protect the Data from a Security Incident please see: https://security.intuit.com/security-practices"
— QuickBooks Time & Workforce (Time/Payroll) DPA
"Disclaimers," "Limitation of Liability," "Indemnity Obligations," "Disputes," and "General Terms (Miscellaneous)"."
— QBO Terms of Service for QuickBooks - US
"We may further modify, suspend or discontinue the Platform at any time. You agree that we will not be liable to you or any third party for any modification, suspensions, or discontinuance of the Platform."
— QBO Terms of Service for QuickBooks - US
"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."
— Global Privacy Statement | Intuit

Arbitration or other dispute resolution process

AI Comment: The playbook's acceptable position requires no limitation as to method of dispute resolution — meaning the customer should retain full access to all dispute resolution options (courts, arbitration, mediation, etc.) without contractual restriction.

The QuickBooks Terms of Service directly and unambiguously conflicts with this requirement. The Disputes section in Section A (Platform Terms) mandates binding arbitration as the exclusive dispute resolution mechanism for all claims arising out of or relating to the Platform or the Agreement, with narrow carveouts only for: (a) small claims court (eligibility-dependent), (b) injunctions or equitable relief "in aid of arbitration," and (c) public injunctive relief (which must be litigated in civil court). These narrow exceptions do not satisfy the playbook's requirement because the general rule — binding arbitration for all substantive claims — remains a severe limitation on dispute resolution method.

Beyond the arbitration mandate itself, the terms impose three additional layered limitations: (1) express waiver of the right to a jury trial; (2) express waiver of participation in class or representative proceedings; and (3) restriction of all claims to individual capacity only. Collectively, these provisions reduce the customer's dispute resolution options to individual-only arbitration or small claims court, foreclosing courts of general jurisdiction, jury trials, and collective/class litigation.

The arbitration clause is governed by the Federal Arbitration Act (FAA) — noted explicitly in the contract and confirmed in the governing jurisdiction pre-computation (California, with FAA overlay for dispute resolution). FAA governance makes this clause highly enforceable and resistant to state-law challenge, including in California, significantly reducing the likelihood that a reviewing attorney could rely on statutory or case-law exceptions to avoid it in a commercial (B2B SaaS) context.

Document hierarchy was examined across all provided documents: Section B Terms prevail over Section A Terms (ToS §Section B intro), but Section B contains no dispute resolution clause that would modify or override Section A's arbitration mandate. The QBO DPA takes precedence over the Agreement per DPA §11.3, but the DPA contains no dispute resolution clause and expressly defers governing law (and by extension, dispute resolution) back to the Agreement (DPA §11.6). The Time/Workforce DPA (Document 4) similarly contains no competing dispute resolution terms. Accordingly, no superseding provision in any higher-precedence document neutralizes or modifies the arbitration clause.

Classification: RED. The contract imposes mandatory binding arbitration — a direct, material conflict with the acceptable position requiring no limitation on dispute resolution method. At Medium weight, this constitutes moderate risk requiring documented justification per the Risk Matrix.

— Superseding reasoning —
The QBO DPA (Document 3, §11.3) takes precedence over the Agreement in conflicts, and Section B Terms take precedence over Section A Terms per the ToS Section B introductory clause. However, neither the DPA nor Section B contains any dispute resolution clause that would modify or supersede the mandatory arbitration provision in Section A of the Terms of Service. The DPA expressly defers its governing law to the Agreement's provisions (DPA §11.6), confirming the ToS arbitration clause continues to govern. The Time/Workforce DPA (Document 4) likewise contains no competing dispute resolution terms. The mandatory arbitration clause in Section A therefore remains operative and unmodified across the full document set. No superseding pair exists.
"Disputes," and "General Terms (Miscellaneous)"."
— QBO Terms of Service for QuickBooks - US
"You agree that the U.S. Federal Arbitration Act governs the interpretation and enforcement of this arbitration provision, and that you and Intuit are each waiving the right to a trial by jury or to participate in a class action."
— QBO Terms of Service for QuickBooks - US
"You and Intuit agree that each may bring Claims against the other only in your or its individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding"
— QBO Terms of Service for QuickBooks - US
"This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the

Agreement, unless required otherwise by applicable Data Protection Laws."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Subprocessor Audit Rights

AI Comment: The playbook item requires a direct customer right to audit Subprocessor systems and their compliance with the DPA. The documents address subprocessor oversight, but in a materially weaker form than the playbook requires: all audit rights run to Intuit itself, not to Subprocessors directly.

What the documents provide:

Both the QBO DPA (Document 3) and the Time/Workforce DPA (Document 4) establish a tiered subprocessor oversight framework:
- Intuit must impose data protection obligations on Subprocessors that are equivalent to those in the applicable DPA.
- Intuit remains fully responsible for Subprocessors' compliance and bears liability for their acts or omissions.
- Customer may submit audit questions or review security audit reports — but these rights are directed at Intuit's own processing and security practices, not at the Subprocessors themselves.

What the documents do not provide:

Neither DPA grants the customer a direct right to audit Subprocessors' systems, inspect their controls, or independently verify their DPA compliance. The customer's only recourse is to audit Intuit, which then bears contractual accountability downstream.

Three additional limitations compound the gap:

1. **Confidentiality carve-out (QBO DPA §3.2):** Intuit expressly acknowledges it "may be prevented from disclosing Sub-processor agreements to Customer due to confidentiality restrictions." This further narrows the customer's visibility into actual Subprocessor arrangements.

2. **SCC substitution (QBO DPA §3.2):** Intuit has contractually substituted SCC Clause 9 compliance with its own Section 3 framework. This forecloses any argument that the incorporated SCCs independently create a stronger Subprocessor audit right for the customer.

3. **Frequency cap (Time/Workforce DPA §2.11):** The audit right over Intuit itself is capped at once per year and is limited to written questions about Intuit's security practices — a notably narrow mechanism even for Intuit-level oversight.

Classification rationale:

This is YELLOW, not RED, because the subprocessor oversight topic is genuinely addressed: Intuit must have compliant sub-processing agreements, remains accountable for Subprocessor performance, and the customer can surface concerns through Intuit. However, the protection is categorically weaker than the playbook's acceptable position, which requires a direct audit right over Subprocessor systems and compliance. The two DPAs are consistent in their approach, and no document in the set provides the direct audit right required. Weight is Medium, yielding a YELLOW risk posture per the risk matrix — documented justification recommended.

— Superseding reasoning —
The QBO DPA (Document 3) and the Time/Workforce DPA (Document 4) govern different service lines and are not in direct conflict with each other; both are applicable and both independently reach the same conclusion. Within the QBO DPA, Section 3.2 and Section 5 are complementary provisions (subprocessor contracting obligations vs. customer audit rights over Intuit, respectively) and do not contradict each other. No superseding determination is required between any pair of PIFs.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Business Connection Data as those…"
2. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"
3. "Intuit shall respond to any written audit questions related to Intuit's security practices submitted to it by Customer, provided that Customer shall not exercise this right more than once per year."

"Intuit imposes data protection terms on any Subprocessor it appoints that are consistent with the terms of this DPA; and

Intuit remains fully liable for any breach of this Clause that is caused by an act, error or omission of its Subprocessor that is acting on our behalf under this DPA."
— QuickBooks Time & Workforce (Time/Payroll) DPA

Cyber Risk Insurance

AI Comment: The vendor's entire publicly-available document set — Terms of Service (Section A and Section B), Global Privacy Statement, QuickBooks Online Data Processing Agreement, QuickBooks Workforce and Time DPA, Intuit Telecom Specific Terms, and Acceptable Use Policy — is completely silent on the subject of cyber risk insurance. No provision addresses: (1) whether Intuit maintains cyber risk insurance; (2) coverage scope (first-party or third-party); (3) coverage limits; (4) additional insured status for customers; or (5) waiver of subrogation. This finding was confirmed by exhaustive review across all six documents in the set.

Under the Review Specific Playbook silence-handling framework, the item weight is Medium, which defaults to a YELLOW classification. No statutory downgrade is warranted: California law (the governing jurisdiction) imposes no requirement on SaaS vendors to maintain or disclose cyber liability insurance in their customer-facing terms. An industry-norm downgrade was considered and rejected for the following reasons:

1. Liability cap exposure: The ToS imposes an aggregate liability cap of the greater of fees paid in the prior 12 months or $100 (§ "Limitation of Liability"). This is an extremely low ceiling. Cyber insurance — and specifically, additional insured status — would be the primary meaningful recovery mechanism for the reviewing organization in a significant breach scenario involving financial data. The low liability cap makes practical risk elevated, not low.

2. Nature of data processed: QuickBooks is deployed to manage bookkeeping, payroll, income/expense tracking, and financial reporting. The platform processes sensitive financial and tax information, and Intuit explicitly acknowledges processing payroll tax data, employee bank account details, and business financial records. A cyber incident affecting this data creates material first-party and third-party harm exposure.

3. Absence of insurable commitments: While Intuit references security measures in the DPA (§4) and its Security Center, contractual security commitments and insurance coverage are distinct obligations. The former addresses prevention; the latter addresses post-incident loss recovery.

While it is industry-standard practice for consumer/SMB SaaS vendors to exclude insurance obligations from publicly-posted Terms of Service — reserving such provisions for negotiated enterprise MSAs — that norm does not reduce the practical risk in this case given the financial sensitivity of the data, the very low contractual liability cap, and the total absence of any additional insured or waiver of subrogation commitment. Accordingly, the classification remains YELLOW. The ideal preference ("e$5M coverage, additional insured designation, waiver of subrogation) is not met on any dimension — the contract is fully silent. Recommend requesting written confirmation from Intuit that it maintains cyber liability insurance, including coverage limits and scope, as a condition of onboarding or via a side letter / order form amendment.

Assignment

AI Comment: The acceptable position requires: (1) both parties may freely assign to successors in interest via merger or acquisition without consent; and (2) any other assignment by Vendor (Intuit) requires the customer's prior consent.

The ToS deviates from this position in two material respects:

First, Intuit's assignment right is completely unconstrained: "Intuit may assign or transfer this Agreement to any party at any time without notice to you." This goes well beyond M&A successors — Intuit can assign to any third party, for any reason, without consent and without even notifying the customer. The acceptable position would require Intuit to obtain the customer's prior consent before making any non-M&A assignment. The ToS eliminates that consent right entirely.

Second, the customer's assignment right is more restricted than the acceptable position contemplates: "You may not assign your rights under this Agreement, by operation of law or otherwise, without our consent." A merger or acquisition of the customer would likely involve an assignment "by operation of law," meaning the customer cannot freely assign even to an M&A successor without Intuit's consent. The acceptable position would permit such transfers freely.

Both deviations are explicit conflicts with the acceptable position — not mere ambiguities. Because the weight is Acceptable to Deviate, the practical risk impact is limited (noted; comment recommended), but the contractual language affirmatively contradicts both prongs of the acceptable position.

— Superseding reasoning —
The Section B Product Specific Terms state they prevail over Section A in the event of direct conflict, but Section B contains no assignment clause. Accordingly, the Section A "Assignment" provision governs without modification. The DPA (Document 3, §11.3) establishes that SCCs > DPA > Agreement in order of precedence for DPA matters, but the DPA also contains no independent assignment clause; §11.5 references "permitted assignees" only in the context of DPA enforcement rights, not as an independent assignment grant or restriction. No superseding determination is therefore required — the ToS Assignment clause is the sole operative provision across all documents.

> *"Intuit may assign or transfer this Agreement to any party at any time without notice to you. You may not assign your rights under this Agreement, by operation of law or otherwise, without our consent. Any attempts to do so without our consent will be void."*
> — QBO Terms of Service for QuickBooks - US

Compliance with Referenced Laws

AI Comment: The documents impose an extensive, multi-statute array of compliance obligations on the customer across at least fifteen distinct legal frameworks, spanning five of the six provided documents. (The Global Privacy Statement describes Intuit's own data practices and imposes no direct compliance obligations on the customer.) Per the playbook instruction, every PIF is classified YELLOW because whether the reviewing organization can abide by any given obligation is not determinable from the documents alone and requires reviewer confirmation.

The twenty-three PIFs span the following compliance obligation categories:

(1) BROAD "ALL APPLICABLE LAWS" MANDATES — Workforce Services (ToS Part F §2.a) impose a sweeping mandate covering all business operations, worker management, and platform use. The Acceptable Use Policy imposes an independent general compliance obligation for payment services.

(2) DATA PROTECTION LAWS (CCPA, GDPR, etc.) — Four separate obligations: the QBO DPA §2.5 general warranty of compliance with all Data Protection Laws; the Workforce/Time DPA §2.1 mandate (which defines "Applicable Data Protection Law" to include employee monitoring laws, wiretap laws, and device location-tracking laws in addition to privacy statutes); the ToS Section A personal information compliance representation for inputting third-party data; and the QBO DPA Annex B US-specific CCPA/US Data Protection Laws compliance obligation.

(3) EXPORT CONTROLS AND SANCTIONS — Three overlapping obligations: ToS Section A (platform-wide EAR/ITAR compliance), Money Movement Terms (Part A service-specific sanctions compliance), and Contractor Payments Terms (Part I, explicitly naming OFAC).

(4) USA PATRIOT ACT / BANK SECRECY ACT — Money Movement Terms cite these statutes as the basis for KYC/AML information-gathering requirements to which the customer must cooperate.

(5) NACHA OPERATING RULES — Two service-module-specific obligations: Money Movement (Part A) for payroll/vendor ACH disbursements and QuickBooks Payments (Part N) for customer-payment ACH transactions. Both require NACHA-compliant consent processes; NACHA may amend rules at any time, creating a rolling compliance obligation.

(6) PCI DSS — QuickBooks Payments (Part N) requires the customer to implement data security policies and physical/electronic controls fully compliant with Payment Card Industry Data Security Standards, potentially requiring formal assessments.

(7) CARD NETWORK RULES — QuickBooks Payments (Part N) requires compliance with Visa, Mastercard, Amex, Discover, and other network rules. Notably, where network rules conflict with Intuit's own terms, network rules take precedence, adding further compliance uncertainty.

(8) ERISA, INTERNAL REVENUE CODE, AND HIPAA — Benefits Administration (Part F §9.c) explicitly assigns ERISA, IRC, and HIPAA compliance responsibility to the customer, along with all required IRS and DOL filings.

(9) TCPA, TSR, AND CTIA GUIDELINES — Third-Party Messaging Services (Section B §6) require compliance with the Telephone Consumer Protection Act, the Telemarketing Sales Rule, and CTIA industry guidelines for all outbound SMS/MMS communications sent to employees, customers, or vendors through the platform.

(10) FCRA — Income/Employment Verification Services (Part F §11) share worker employment and income data with Equifax Workforce Solutions for disclosure under the FCRA, implicating the customer's ongoing FCRA furnisher obligations.

(11) FEDERAL/STATE PAYROLL TAX LAWS — Workforce (Part F §3.d) retains ultimate payroll tax filing and payment responsibility with the customer regardless of Intuit's assistance.

(12) ANTI-DISCRIMINATION, EMPLOYMENT ELIGIBILITY, AND SALARY POSTING LAWS — Job Postings (Part F §8.a) require compliance with Title VII, ADEA, ADA, GINA, IRCA, and state salary-range posting laws.

(13) BIOMETRIC DATA LAWS — Both DPAs (QBO DPA §2.4 and Workforce/Time DPA §2.12.1) independently allocate biometric data compliance to the customer. Where both services are used concurrently, both obligations operate in parallel.

(14) STATE/FEDERAL TIME-TRACKING LAWS — QuickBooks Time (Part H) places sole responsibility for wage/hour and timekeeping-law compliance on the customer.

(15) PRIVACY NOTICE DISCLOSURE OBLIGATION — ToS Section B §7 requires the customer to update its external privacy notice to disclose Intuit's data controller role and to link to Intuit's Global Privacy Statement.

DOCUMENT HIERARCHY NOTE: Section B Terms expressly prevail over Section A Terms in cases of conflict (ToS §1.225). The QBO DPA prevails over the ToS for data processing conflicts in the following order: SCCs !' QBO DPA !' Agreement (QBO DPA §11.3). The Workforce/Time DPA similarly prevails over the Agreement for data processing matters. This hierarchy does not eliminate any compliance obligation identified; all obligations identified remain additive and operative.

PREFERENCE ASSESSMENT: The stated preference — no compliance obligations beyond laws applicable to the

customer's own use of the services — is not met. Multiple obligations (PCI DSS, NACHA Rules, card network rules, ERISA, HIPAA, FCRA, TCPA, biometric data laws) go materially beyond laws that apply merely because one uses accounting software. They reflect obligations typically borne by regulated financial services entities, employers, and health benefit plan sponsors. The most operationally significant obligations for a bookkeeping/payroll SaaS customer are likely: ERISA/HIPAA (benefits), PCI DSS (card payments), NACHA (ACH), and TCPA/CTIA (employee/vendor messaging). Each warrants targeted reviewer attention.

— Note —
The AI cited 10 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "You are solely responsible for determining whether the Workforce Services meet your business's needs, and for ensuring that the operation of your business, the management of your Workers, and your use…"
2. "To the extent we allow you to input personal information (as the term is defined under applicable law) about other individuals other than yourself, you represent and warrant that you have complied wit…"
3. "In order to comply with applicable federal laws relating to anti-money laundering and terrorism financing, including the USA PATRIOT Act and the Bank Secrecy Act, IPI may request that you provide info…"
4. "For Payees that will receive disbursements via ACH, you agree to obtain the Payee's consent to credit their bank account and initiate a disbursement over the ACH network. Such consent must be in a for…"
5. "You must ensure you have data security policies and processes in place to protect cardholder and payor payment information in compliance with PCI DSS and NACHA security requirements. You must keep all…"
6. "To the extent anything in these QuickBooks Payments Terms conflict with an applicable card or payment network rule (such as VISA, MasterCard, American Express, Discover, or NACHA) (collectively, the "…"
7. "You agree that the business and personal information provided in connection with your use of Workforce Services, including income and employment information of your current or former Workers (collecti…"
8. "Customer recognizes and agrees that there are various laws that specifically govern the collection, use, and retention of Biometric Data, and understands that it is Customer's responsibility to comply…"
9. "You accept sole responsibility for ensuring that you and your Workers' use of Time is in compliance with state and federal laws and reporting obligations."
10. "You further agree that you will notify Business Connection Data subjects in your privacy notice or by other commercially reasonable means, that Intuit is a data controller with respect to Business Con…"

> *"You are independently responsible for complying with applicable laws and our policies."*
> — Acceptable Use Policy (payments / money movement)

> *"Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Business Connection Data and any processing instructions it issues to Intuit; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws and the terms of the Agreement for Intuit to process Business Connection Data for the purposes described in the Agreement."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

> *"Each party shall comply with the obligations that apply to it under Applicable Data Protection Law."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA

> *"Customer is responsible for ensuring that it has complied, and will continue to comply with the requirements of US Data Protection Laws in its use of the Services and its own processing of personal data."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

> *"you will not use, export, re-export, import, sell, release, or transfer the Platform, the Software or the Service directly or indirectly, except as authorized by United States law, the laws of the jurisdiction where the Platform and Software are made available, and any other applicable laws and regulations."*
> — QBO Terms of Service for QuickBooks - US

> *"You must comply with applicable export control and sanctions laws and regulations, and will not transfer or provide any part of the Services, in violation of these laws and regulations, directly or indirectly."*
> — QBO Terms of Service for QuickBooks - US

> *"You assume sole responsibility for, and will ensure that your payment information, Content, data, documents or materials used, disclosed, entered into or created using the Contractor Payments Services are accurate, reliable and complete, do not violate the Agreement, and comply with the Office of Foreign Assets Control of the U.S. Treasury and all other applicable laws or regulations."*
> — QBO Terms of Service for QuickBooks - US

> *"Specific to NACHA Rules, you agree to obtain customer consent to debit or credit their bank account and initiate a transaction over the ACH network. Such consent must be in a form and manner that complies with NACHA Rules and the documentation for ACH transactions."*
> — QBO Terms of Service for QuickBooks - US

> *"making all required filings with governmental agencies, including the IRS and Department of Labor; and (viii) ensuring the legal and tax status of your Plans, including compliance with respect to the Internal Revenue Code, ERISA, and HIPAA, as applicable."*
> — QBO Terms of Service for QuickBooks - US

> *"You represent and warrant that the owners, which shall include the subscriber and/or authorized user(s), of the phone numbers to which you transmit outbound text messages through the Platform have expressly consented or otherwise opted-in to the receipt of such messages, in accordance with the Telephone Consumer Protection Act, the Telemarketing Sales Rule, and other applicable federal, state, local laws, statutes and regulations, and industry guidelines and best practices, including, but not limited to, the CTIA Short Code Monitoring Handbook and the CTIA Messaging Principles & Best Practices"*
> — QBO Terms of Service for QuickBooks - US

> *"You are responsible for the timely filing of your payroll tax returns and the timely payment of payroll taxes for your employees, even if you have authorized us to file the returns and make the payments."*

— QBO Terms of Service for QuickBooks - US

"Job Posting content must comply with all applicable federal, state, and local laws, including anti-discrimination, labor and employment, equal opportunity, employment eligibility, and salary range posting requirements. At a minimum, Job Postings must (i) not contain any requirement that unlawfully discriminates based on race, sex, age, physical or mental disability, religion, national origin, citizenship, military or veteran status, genetic information, or any other legally protected characteristic, and (ii) not exclude applicants based on criminal history, unless such exclusion is a legally permissible, legitimate job requirement or required by law."

— QBO Terms of Service for QuickBooks - US

"You recognize and agree that there are various laws that specifically govern the collection, use, and retention of Biometric Data, and understand that it is your responsibility to comply with all applicable laws, including Applicable Data Protection Law."

— QuickBooks Time & Workforce (Time/Payroll) DPA

Regulatory Disclosure Procedure

AI Comment: The playbook item requires that upon receiving a regulatory or legal authority request, Intuit must: (1) forward or notify the customer of the request (unless prohibited by law), and (2) await customer instructions before acting on the request. Analysis across all provided documents reveals this protection is critically absent for US/California customers — the governing jurisdiction for this review.

EU/UK DPA Provision — Exists But Is Not Applicable to Governing Jurisdiction: The QuickBooks Online DPA Annex B contains an explicit government data access notification procedure that directly addresses the playbook scenario. When Intuit receives a compulsory government/law enforcement request, it must: (i) review legality; (ii) inform the agency that Intuit is a processor; (iii) redirect the agency to the customer; (iv) notify the customer by email to allow seeking a protective order; and (v) provide only minimum permissible information. A prohibited-by-law carve-out is included, and Intuit must seek waivers of notification prohibitions where legally barred from notifying. However, this procedure is expressly and exclusively limited to customers "whose primary contact information indicates the Customer is located in Europe." No US analog exists anywhere in the document set. Importantly, even if this provision applied, it does not require Intuit to await customer instructions before responding — it permits providing minimum information while the customer seeks a protective order — meaning this provision would be YELLOW rather than GREEN under the playbook's acceptable position even if it applied.

DPA US Annex B Terms — Absence of Protection: The DPA Annex B US-specific section addresses only CCPA Service Provider obligations: purpose limitation, restrictions on selling/sharing Business Connection Data, data subject request handling, and CCPA compliance. There is no government or regulatory authority data access notification requirement in the US section, confirming the omission is deliberate rather than an oversight.

DPA Hierarchy Does Not Rescue the Gap: Per DPA Section 11.3, the DPA takes precedence over the Agreement (ToS) in cases of conflict. However, the DPA is itself silent on government data access notification for US customers. With the DPA silent, the Agreement's provisions fill the gap — and those provisions (ToS + Privacy Statement) permit unilateral disclosure without customer notification.

ToS and Privacy Statement — Affirmative Contrary Provisions: Both the Terms of Service (Section A — Prohibited Uses) and the Global Privacy Statement affirmatively reserve Intuit's right to disclose information to comply with legal obligations, subpoenas, court orders, and regulatory processes — with no requirement to notify the customer first or await instructions. These provisions run directly contrary to the playbook's acceptable position.

Conclusion: The vendor has constructed a jurisdiction-differentiated disclosure regime: European customers receive a substantive government data access notification procedure; US customers receive none, and are instead subject to affirmative unilateral disclosure rights. For the governing jurisdiction (California/United States), the playbook requirement is not met — this is RED for a High-weight item, requiring senior legal justification to proceed.

— Note —

The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.

1. "As a matter of general practice, Intuit does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Intuit accounts (including Busin…"

"We may disclose any information necessary to satisfy our legal obligations, protect Intuit or its customers, or operate the Platform properly."

— QBO Terms of Service for QuickBooks - US

"We may share your personal information with third parties for legal reasons without your consent, and as permitted by law, including:

- When we reasonably believe disclosure is required in order to comply with a subpoena, court order, or other applicable law, regulation or legal process;
- To protect the rights, property, or safety of Intuit, TurboTax, the Intuit Platform, our customers or others;
- To protect or defend against attacks;
- To enforce, remedy, or apply our Terms of Service or other agreements;
- To prevent fraud, cybersecurity attacks or illegal activity;
- For debt collection; and
- With regulatory agencies, including government tax agencies, as necessary to help detect and combat fraud and/or protect our customers, users and/or the Intuit Platform, or in required institutional risk control programs."

— Global Privacy Statement | Intuit

Encryption in Transit

AI Comment: The playbook item requires confirmation that data is encrypted in transit using TLS 1.2 or higher, or then-current industry-standard transport encryption. Across all documents in the review set, Intuit addresses the topic of data security and encryption, but nowhere specifies TLS 1.2 or higher — or any named transport encryption protocol — as the standard governing transit protection.

The strongest contractual commitment appears in the QBO DPA (§4.1), which lists "pseudonymisation or encryption of personal data" as one of several security measures Intuit "shall include, as appropriate." This language is qualified ("as appropriate"), does not isolate in-transit encryption as distinct from at-rest encryption, and does not name a protocol or version. The Time/Workforce DPA (§2.5) mirrors this formulation. The Terms of Service Data Transfer Service clause commits to "appropriate technical and organizational measures to secure this data consistent with applicable data privacy and protection laws or regulations" — again general, unspecified, and not transport-encryption-specific. One ToS provision confirms an "encrypted, secure connection" for 1099 data transmitted to TurboTax servers, but that is feature-scoped and protocol-unspecified. The Global Privacy Statement states only "reasonable physical, technical and organizational safeguards."

Detailed security specifications are deferred to external resources (Intuit Security Center at security.intuit.com and security.intuit.com/security-practices), which are referenced in the DPA but were not provided in this document set and cannot be cited as evidence. Accordingly, the governing language — the QBO DPA §4.1 (which prevails over the ToS per the DPA's §11.3 hierarchy clause) — acknowledges encryption as a relevant measure but does not commit to TLS 1.2 or any equivalent industry-standard transit protocol.

For a HIGH weight item requiring explicit TLS 1.2+ (or equivalent) confirmation in transit, this constitutes a topic-addressed but standard-unconfirmed finding. The protection is arguably present in practice (Intuit is a large financial-technology vendor where TLS 1.2+ is near-universal), but the contractual text does not provide the verifiable commitment the playbook requires. Classification: YELLOW — the same topic is addressed through general security and encryption language, but the specific technical threshold (TLS 1.2 or higher, or named industry standard) cannot be confirmed from the document set.

— Superseding reasoning —
The QBO DPA (Document 3) contains an explicit document-hierarchy clause at §11.3 stating that, in any conflict or inconsistency, provisions prevail in this order: (i) SCCs, (ii) the DPA, and (iii) the Agreement (Terms of Service). Accordingly, the DPA's §4.1 security-measures language is the governing standard for Business Connection Data security obligations — including any transit-encryption commitment — and supersedes the more general security language in the ToS Data Transfer Service clause. The Time/Workforce DPA (Document 4) similarly governs over the Agreement for Customer Data processed under those services (per the DPA's introductory "How this DPA applies" section). Where both DPAs address the same general security standard, their language is substantively identical ("appropriate technical and organizational measures"); neither refines nor narrows the other.

> *"We will use appropriate technical and organizational measures to secure this data consistent with applicable data privacy and protection laws or regulations."*
> — QBO Terms of Service for QuickBooks - US
>
> *"1099 data will be transmitted via an encrypted, secure connection to the TurboTax® servers for automatic download into TurboTax®"*
> — QBO Terms of Service for QuickBooks - US
>
> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
>
> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA
>
> *"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information."*
> — Global Privacy Statement | Intuit

Subprocessor Agreements

AI Comment: The playbook item contains two distinct, independently assessable requirements: (1) written agreements with subprocessors that are at least as strict as the DPA; and (2) prior approval or prohibition for subprocessors with privileged access. The documents address the first requirement substantively but fall short on precision; the second requirement is wholly absent, replaced by the opposite approach — blanket upfront customer consent.

First Prong — Written Agreements At Least As Strict as the DPA:
Both DPAs engage this requirement. The QBO DPA (§3.2) requires Intuit to enter into a written agreement with each Sub-processor containing data protection obligations that "provide at least the same level of protection for Business Connection Data as those in this DPA." This nominally satisfies the acceptable position. However, the appended qualifier — "to the extent applicable to the nature of the service provided by such Sub-processor" — introduces discretionary flexibility that could allow Intuit to impose reduced obligations on subprocessors it characterizes as providing limited-scope services. This is a weaker standard than the unconditional "at least as strict as this DPA" the playbook requires. The Workforce/Time DPA (§2.6) goes further in the wrong direction, requiring only that data protection terms be "consistent with" the DPA — a materially lower bar than "at least as strict." Critically, the QBO DPA also explicitly acknowledges that actual sub-processor agreements may be withheld from the customer due to confidentiality restrictions, limiting the practical ability to audit compliance with the protection-standard commitment.

Second Prong — Prior Approval or Prohibition for Privileged-Access Subprocessors:
This requirement is not met in any document across the entire set. Both DPAs grant blanket, upfront customer authorization for Intuit to engage any sub-processor, subject to the general conditions of §3.2/§2.6. There is no category of "privileged access" subprocessors identified, no prior-approval right for the customer with respect to any individual subprocessor engagement, and no prohibition mechanism. The only customer remedy upon objecting to a specific subprocessor is to terminate the entire Agreement (with fees due through the termination date) — the opposite of targeted, access-based control. For a SaaS platform processing highly sensitive financial data (bookkeeping records, payroll, income and expense data, tax filings), the complete absence of a privileged-access gating mechanism is a material and meaningful gap against a Critical-weight playbook item.

Overall: The topic of subprocessor agreements is addressed and written agreements are required, preventing a RED classification. However, the protection standard includes materially weakening qualifiers ("to the extent applicable"; "consistent with"), the prior-approval/prohibition mechanism is wholly absent, and transparency into actual sub-processor agreement terms is contractually limited. The combined effect is a contract that addresses the topic with materially weaker protection than the playbook's acceptable position requires — a YELLOW classification with heightened practical risk given Critical weight. Per the risk matrix, this requires review and documented assessment before acceptance.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Business Connection Data as those…"
2. "If Customer refuses to consent to Intuit's appointment of a third-party Subprocessor relating to the protection of the Customer Data, Customer may elect to suspend or terminate the Agreement, includin…"

> *"Customer hereby authorizes Intuit or any member of the Intuit Group on behalf of/for the benefit of Intuit to engage Sub-processors, in accordance with Section 3.2, to assist Intuit in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Intuit may be prevented from disclosing Sub-processor agreements to Customer due to confidentiality restrictions but Intuit shall, upon request, use reasonable efforts to provide Customer with all relevant information it reasonably can in connection with Subprocessor agreements."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Intuit imposes data protection terms on any Subprocessor it appoints that are consistent with the terms of this DPA; and*
>
> *Intuit remains fully liable for any breach of this Clause that is caused by an act, error or omission of its Subprocessor that is acting on our behalf under this DPA."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA
> *"Where Sub-processors process Business Connection Data, Intuit takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom Intuit has entered into a written contract that includes terms substantially similar to this section of Annex B or are otherwise exempt from the CCPA. Intuit conducts appropriate due diligence on its Sub-processors."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Data Processing Security Policies

AI Comment: The playbook item requires (1) adequate security for data processing systems and (2) adequate policies to prevent unauthorized access to those systems. The document set collectively addresses both prongs, with the most directly governing language found in the QBO Data Processing Agreement (Doc 3) and the QuickBooks Time & Workforce DPA (Doc 4).

Prong 1 — Adequate security for data processing systems: The QBO DPA §4.1 (Doc 3) is the primary governing clause. It commits Intuit to "at a minimum" implement "appropriate technical and organisational measures" and specifically enumerates four security requirements: (a) pseudonymisation or encryption of personal data; (b) ongoing confidentiality, integrity, availability and resilience of processing systems; (c) ability to restore data availability timely after a physical or

technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of security measures. These are precisely the kinds of enumerated controls the playbook item contemplates. The Time/Workforce DPA §2.5 (Doc 4) contains corroborating language for payroll/time-tracking data specifically.

Prong 2 — Adequate policies to prevent unauthorized access: The QBO DPA §4.2 (Doc 3) requires all persons authorized by Intuit to process Business Connection Data — including staff, agents, and subcontractors — to be under an "appropriate obligation of confidentiality." The Time/Workforce DPA §2.4 (Doc 4) strengthens this further, imposing a "strict duty of confidentiality" on Authorized Persons and prohibiting any person not under that duty from processing Customer Data. These confidentiality-of-processing provisions directly implement access control at the personnel layer.

Audit and Transparency: The QBO DPA §5 (Doc 3) provides access to security audit reports and allows written questions to be submitted, enabling the Customer to verify compliance. The Time/Workforce DPA §2.11 (Doc 4) also provides audit rights but restricts them to written questions no more than once per year, which is a limitation relative to best practice.

Superseding conflict — ToS security disclaimer: The ToS Disclaimers section (Doc 1) states Intuit does not warrant the Platform is "secure," which would be a RED finding in isolation. However, DPA §11.3 (Doc 3) explicitly establishes the DPA takes precedence over the Agreement in the event of conflict, and the ToS §B preamble states Section B Terms prevail over Section A Terms. Accordingly, the DPA's affirmative security obligations supersede the general ToS warranty disclaimer for data processing matters.

Privacy Statement (Doc 2): Uses softer "reasonable physical, technical and organizational safeguards" language with a qualification that security "cannot completely" be ensured. This is weaker than the DPA's "appropriate measures" with enumerated specifics, and classified YELLOW. For data processing under the DPAs, the DPA language is controlling.

Limitations noted (not determinative):
- Detailed security policies are referenced at external URLs (security.intuit.com / security-practices) rather than reproduced in full within the contract. This is common SaaS practice but requires the Customer to independently verify.
- Audit rights are limited: once per year, written questions only (Time/Workforce DPA §2.11).
- Shared responsibility model: Customer retains responsibility for securing account credentials and data in transit (DPA §4.5).
- DPA §4.3 shifts a verification obligation to Customer to independently assess whether security measures meet their requirements.

These limitations are operational and do not negate the core adequacy of Intuit's contractual security commitments. Both prongs of the playbook item are met by the DPA provisions, which govern data processing and take precedence over the general ToS disclaimer. Classification: **GREEN**, confidence: **HIGH**.

— Superseding reasoning —
The QBO DPA §11.3 (Doc 3) expressly establishes that in the event of any conflict or inconsistency between the DPA and the Agreement (Terms of Service), the DPA prevails. Additionally, the ToS §B preamble (Doc 1, §1-225) confirms that Section B Terms prevail over Section A Terms. The ToS §A Disclaimers section (Doc 1) disclaims that the Platform is warranted to be "secure" — a provision that directly conflicts with the DPA's affirmative commitment in §4.1 to implement enumerated security measures. Pursuant to the DOCUMENT_HIERARCHY established by DPA §11.3, the DPA's security obligations are the governing language for data processing activities, and the ToS security disclaimer is superseded for that scope. The governing language after applying this precedence is DPA §4.1's commitment to appropriate technical and organizational measures including pseudonymization/encryption, confidentiality/integrity/availability/resilience, disaster recovery, and regular testing.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"
2. "Intuit shall ensure that any person that it authorizes to Process the Customer Data (including Intuit's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of …"
3. "Intuit shall respond to any written audit questions related to Intuit's security practices submitted to it by Customer, provided that Customer shall not exercise this right more than once per year."

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."
— QuickBooks Time & Workforce (Time/Payroll) DPA
"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."
— Global Privacy Statement | Intuit
"We do not warrant that the Platform is error-free, secure, or free from any viruses or other harmful components."
— QBO Terms of Service for QuickBooks - US
"We will use appropriate technical and organizational measures to secure this data consistent with applicable data privacy and protection laws or regulations."
— QBO Terms of Service for QuickBooks - US

Processing Limitation

AI Comment: The QuickBooks document set contains dedicated purpose limitation provisions in two Data Processing Agreements (the QBO DPA and the Workforce/Time DPA) that partially satisfy the acceptable position. The QBO DPA § 2.2 constrains Intuit's processing of "Business Connection Data" (customer's customers, employees, vendors, prospects) to "Customer's documented lawful instructions" — a direct textual match to the acceptable position's requirement that processing be limited to contractual obligations and written instructions. The Workforce/Time DPA § 2.2 similarly requires Intuit to process "strictly in accordance with the documented instructions of Customer." These provisions, combined with the DPA's explicit document hierarchy clause (§ 11.3, which establishes DPA > Agreement in any conflict), provide meaningful protection for Business Connection Data when Intuit acts as processor. For Workforce/Time services, additional CCPA-specific restrictions (§ 3.1) further bar Intuit from using or disclosing Personal Information outside the parties' direct business relationship.

However, three material weaknesses prevent a GREEN finding for this Critical-weight item:

1. **Controller Carve-out (QBO DPA § 2.1 / ToS Section B § 7):** Both the QBO DPA and the ToS explicitly acknowledge that Intuit acts as an independent data controller — not a processor — when using Business Connection Data for product development, data analytics, fraud prevention, and marketing. When Intuit acts as controller, it processes pursuant to its own Global Privacy Statement, not per customer instructions. This carve-out is self-contained within the DPA itself (§ 2.1 is an explicit exception to § 2.2) and cannot be resolved by document hierarchy.

2. **AI Model Training and Broad Product Development (Privacy Statement):** Intuit's Global Privacy Statement — the governing document for its controller activities — explicitly includes training AI/ML models, conducting data analytics for product insights, and marketing as permitted uses of personal information. QuickBooks data (financial transactions, payroll details, business income and expenses) is within the scope of data processed for these controller purposes with no customer instruction required.

3. **Unrestricted Use of Deidentified/Aggregated Data (ToS Section A — Content and Data):** The ToS grants Intuit unrestricted rights to use deidentified and aggregated data derived from customer content for any purpose including marketing — explicitly stating this data "may be used without restriction." This provision is not governed by the DPA (which covers Business Connection Data, a distinct category from the customer's own content) and therefore is not superseded by the DPA's purpose limitation.

The DPA purpose limitation constitutes the governing language for Business Connection Data when Intuit acts as processor, and the DPA's document hierarchy clause ensures it prevails over conflicting ToS provisions in that domain. However, the explicit controller carve-out for marketing and AI/product development — consistent across the DPA, ToS, and Privacy Statement — represents a material departure from the acceptable position that processing be limited to contractual obligations and written instructions. For a SaaS platform processing sensitive financial data including payroll, income, and custom financial reports, this is a meaningful gap that requires documented assessment.

— Superseding reasoning —
The QBO DPA § 11.3 establishes an explicit document hierarchy: SCCs > DPA > Agreement (Terms of Service). To the extent the ToS "Agreement to These Terms" provision — which frames cross-platform data sharing for marketing as an instruction given by the customer upon use of the Platform — could be read to authorize broader processing of Business Connection Data beyond contractual obligations, the QBO DPA § 2.2 purpose limitation overrides it for that data category. The governing language for Business Connection Data processing is therefore the DPA's purpose limitation clause. This superseding determination does not, however, resolve the controller carve-out in DPA § 2.1 itself, which is not in conflict with any other provision but rather an express exception built into the same document as the purpose limitation.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the

quoted text below against the source manually.
1. "Intuit shall process Business Connection Data, as further described in Annex A (Details of Data Processing) of this DPA, only in accordance with Customer's documented lawful instructions as set forth …"
2. "Intuit may collect, derive or generate deidentified and/or aggregated data regarding your usage of or the performance of the Platform, including data derived from your Content. Intuit will own all suc…"
3. "By using the Platform, you are instructing us to share your data across our Platform for marketing, eligibility, and other purposes described in our Global Privacy Statement, consistent with applicabl…"
4. "When acting as Processor, Intuit shall Process the Customer Data as a Processor only as necessary to perform its obligations under the Agreement and strictly in accordance with the documented instruct…"

> *"the parties acknowledge that Intuit shall be a controller when Intuit uses Business Connection Data for certain limited purposes, as further described in the Agreement (including, for example, in relation to Intuit product development and improvement, data analytics, and fraud prevention and security), for product and service improvement, and to market Intuit's products and services."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"For the purposes of applicable data protection laws, you agree and acknowledge that there are instances in which we process Business Connection Data as a data controller for certain limited purposes, including for example, in relation to our product development and improvement, data analytics, and fraud prevention and security."*
> — QBO Terms of Service for QuickBooks - US
> *"Research and development. We may use your personal information to:**"*
> — Global Privacy Statement | Intuit

No AI/ML Training on Our Data

AI Comment: This Critical-weight playbook item is directly and unambiguously violated across multiple documents. The findings are summarized below in order of severity.

Direct conflict — AI/ML training explicitly authorized (Privacy Statement): The Global Privacy Statement states, within its "Research and development" section, that Intuit uses customer personal information to train "artificial intelligence models and other machine learning models." This is an explicit, unqualified authorization to train generalized AI/ML models on customer data — precisely what the acceptable position prohibits.

Aggregated/deidentified data — unrestricted use (ToS): The Terms of Service authorize Intuit to collect, derive, or generate deidentified and aggregated data from customer Content and use it "without restriction" for improving or marketing Intuit's products and services. This violates the ideal preference, which prohibits even aggregated or anonymized use.

Digital Assistants / AI improvement (ToS): Content submitted to Intuit's Digital Assistants (chatbots, AI agents) may be used to "improve our Platform, Digital Assistants, and related technology" — directly implicating AI/ML system improvement using customer-provided data.

DPA controller exception neutralizes purpose limitation: The QBO Data Processing Agreement contains a processor-role purpose limitation (§2.2) that initially appears protective. However, §2.1 explicitly carves out a separate controller role for Intuit when using Business Connection Data for "product development and improvement, data analytics." When Intuit acts as controller under this exception, the DPA's purpose limitation does not apply; instead, the Global Privacy Statement governs — and the Privacy Statement explicitly permits AI/ML training. The purpose limitation is therefore superseded for all product-improvement uses, including AI training (see Superseding Details).

Workforce Services PI for product improvement (ToS §15): Section B of the ToS (which prevails over Section A per the ToS hierarchy) additionally grants Intuit a royalty-free license over Personal Information processed through Workforce Services and expressly states "Intuit may use the Personal Information to improve Workforce Services and other Intuit products" — reinforcing the AI training risk for payroll/HR data specifically.

Narrow mitigant — Workforce DPA CCPA restriction (partial): The QB Time and Workforce DPA §3.1 restricts use of Workforce-specific Personal Information to "Business Purposes...namely employee and benefits management" and prohibits combining it with third-party data. This is more protective language for payroll data specifically, but (i) it applies only to QB Time/Workforce data, not the core QBO bookkeeping platform, (ii) the Workforce DPA still acknowledges Intuit's controller role which can reintroduce product-improvement uses, and (iii) it does not contain an explicit AI/ML training prohibition.

Negative implication of Google Workspace carve-out: The Privacy Statement carves out Google Workspace API data from AI/ML training, explicitly noting that such data is "not used to develop, improve, or train any generalized AI and/or ML models." The absence of any comparable carve-out for general customer data — combined with the explicit AI training authorization — confirms by negative implication that non-Google-API customer data (i.e., QuickBooks bookkeeping, financial, and payroll data) is used for AI/ML training.

Overall conclusion: The acceptable position (no AI/ML training on customer data except models used solely for the customer) is clearly not met. The ideal preference (no use for any purpose beyond providing services, including aggregated/anonymized form) is also clearly not met. This is a blocking-level finding under the Critical weight / RED risk matrix. Board approval and a documented exception would be required to proceed.

— Superseding reasoning —

Within the QBO Data Processing Agreement, the general processor purpose limitation in §2.2 (PIF index 5) appears to restrict Intuit's use of Business Connection Data to customer-documented instructions. However, §2.1 of the same DPA creates a specific exception: when Intuit uses Business Connection Data for product development and improvement, it acts as an independent data controller, not a processor bound by the purpose limitation. Applying the SPECIFIC_OVER_GENERAL principle, the specific controller carve-out in §2.1 supersedes the general purpose limitation in §2.2 for those product-improvement activities. When acting as controller, Intuit's processing is governed by the Global Privacy Statement rather than the DPA's purpose limitation — and the Privacy Statement explicitly includes training AI/ML models as a permitted use. The DPA's stated precedence over the Agreement (§11.3: SCCs > DPA > Agreement) does not cure this defect, because the DPA itself is the source of the controller exception that enables AI training: there is no conflict between the DPA purpose limitation (processor hat) and the Privacy Statement AI training authorization (controller hat) — they operate in parallel lanes. No other superseding relationship between documents was identified for this playbook item.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Please note any data obtained through Google Workspace APIs is not used to develop, improve, or train any generalized AI and/or ML models. Any data originating from the Google Workspace API is instead…"
2. "Provided, however, that the parties acknowledge that Intuit shall be a controller when Intuit uses Business Connection Data for certain limited purposes, as further described in the Agreement (includi…"
3. "Purpose limitation. Intuit shall process Business Connection Data, as further described in Annex A (Details of Data Processing) of this DPA, only in accordance with Customer's documented lawful instru…"
4. "In your use of the Workforce Services you are hereby granting Intuit a non-exclusive, worldwide, royalty-free right and license to collect, use, copy, display, perform, store, transmit, modify and cre…"
5. "Intuit will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Agreement, …"

> *"Improve and develop our products and services by analyzing how they are used and interacted with, by training our artificial intelligence models and other machine learning models, as well as by assessing the use of and interactions with our Platform and certain content our customers send or display through the Platform, including by conducting data analytics to develop insights about you, your needs, and your preferences, so we can make more informed predictions, recommendations, and products for our customers."*
> — Global Privacy Statement | Intuit
> *"Content and Data"*
> — QBO Terms of Service for QuickBooks - US
> *"Any Content you provide to Digital Assistants may be used to provide more personalized responses and improve our Platform, Digital Assistants, and related technology."*
> — QBO Terms of Service for QuickBooks - US

Modification of Terms

AI Comment: The Intuit/QuickBooks Terms of Service directly addresses modification of terms across multiple provisions, but the overall framework falls short of the acceptable position in one critical respect and clearly does not meet the ideal preference.

Acceptable position analysis:

Accessibility (met): The Terms of Service are publicly posted and carry explicit version dates (Version 02122026 for Section A; Version 05132026 for Section B), satisfying the requirement that the current version be accessible with an updated effective date.

Ascertainability before taking effect (weakly met — YELLOW trigger): The Section A "Changes" provision states that Intuit "may notify you" of modifications by posting to the Platform, website, or "by other means." The word "may" renders notification discretionary, not obligatory. There is no defined advance notice period before general contractual modifications take effect. Continued use of the Platform constitutes acceptance. This construct places the entire burden of monitoring for changes on the customer, meaning a modification to a material term could technically take effect without the customer receiving any direct notification — satisfying the letter of "ascertainability" (changes are posted and findable) but not its spirit (changes are proactively communicated before taking effect). This represents a meaningful gap from the acceptable position.

Ideal preference analysis (not met):

Advance written notice: No advance written notice is required for general T&C modifications. More favorable provisions exist for limited categories — subscription fee/price changes receive some form of notice (no defined period), annual subscription renewals receive a 30–60 day reminder, and QuickBooks Payments rate/fee increases receive 30 days' advance notice — but these do not extend to substantive contractual modifications.

Opportunity to terminate with pro-rata refund: A right to exit by stopping use/terminating the account is available on disagreement with changes (Section A "Changes"). However, the "Payment & Cancellations" section contains an explicit prohibition: "We do not provide refunds or credits for any cancellations or partial subscription period." This directly eliminates the financial remedy contemplated by the ideal preference. A customer who disagrees with a material term change mid-cycle has no mechanism to exit with a pro-rata refund.

Superseding note: The general modification-of-terms provision in Section A governs most changes. For subscription fee/price changes, the more specific Section A "Payment & Cancellations" provisions supersede the general approach (specific-

over-general). For QuickBooks Payments rate/fee changes specifically, Section B Part N's 30-day advance notice requirement supersedes the general Section A subscription price change provision, as Section B terms expressly prevail over Section A for conflicts per the agreement's own hierarchy.

Net classification: YELLOW — The topic is addressed and terms are accessible, but the discretionary notification mechanism without a defined advance notice period for general contractual changes weakens the "must not take effect without being ascertainable" requirement. The ideal preference (advance written notice + pro-rata refund option) is not met. Given the High weight of this item, this finding requires documented legal review and assessment before acceptance.

— Superseding reasoning —
The general modification-of-terms provision in Section A ("Changes") is a catch-all governing all contractual modifications. However, for subscription fee/price changes specifically, the "Payment & Cancellations" provision within the same Section A supersedes the general provision on the specific-over-general principle — the fee change provisions are more detailed and particularized to that scenario. For QuickBooks Payments rate and fee changes specifically, the Section B Part N provision (30 days advance notice) supersedes the general Section A subscription price change provision, because Section B terms expressly prevail over Section A "for any conflict or inconsistency" and the Part N provision is a narrower, product-specific rule within that hierarchy.

> *"We may modify the provisions of this Agreement at any time. We may notify you of such modifications by posting through the Platform or on our website or by other means. It is important that you review this Agreement whenever we modify it because your continued use of the Platform indicates your agreement to the modifications."*
> — QBO Terms of Service for QuickBooks - US
> *"In some cases, you may need to accept changes to this Agreement to continue using the Platform. If you do not agree to the changes, you may stop using the Platform or terminate your account."*
> — QBO Terms of Service for QuickBooks - US
> *"We do not provide refunds or credits for any cancellations or partial subscription period."*
> — QBO Terms of Service for QuickBooks - US
> *"For annual subscriptions, we will send you a reminder with the then-current subscription fee no less than thirty (30) days and no more than sixty (60) days before your subscription term ends, or otherwise as required by applicable law."*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit may change the price for recurring subscription fees from time to time with notice to you. Price changes will take effect at the start of the next subscription period following the date of the price change. If you do not agree with the price change, you may unsubscribe prior to the price change going into effect."*
> — QBO Terms of Service for QuickBooks - US
> *"All rates and fees are in U.S. dollars and subject to change; where you may become subject to any increase in rates or fees, we will provide thirty (30) days advance notice. We may provide you notice by posting updated pricing or terms on our website or sending you email communication. Notwithstanding anything to the contrary in the Section A Terms, price changes are effective on the date indicated on our notice or posted terms."*
> — QBO Terms of Service for QuickBooks - US
> *"From time to time we may change or update our Privacy Statement. We reserve the right to make changes or updates at any time. If we make material changes to the way we process your personal information, we will notify you by posting a notice in the Intuit Platform or on a community post; by sending you a notification; or by other means consistent with applicable law."*
> — Global Privacy Statement | Intuit

Breach Notification Timeline

AI Comment: The playbook's acceptable threshold requires breach notification (i) "without undue delay, and in any event within 72 hours," (ii) for both actual and suspected Data Security Breaches, and (iii) for any actual or potential breach of the DPA. The ideal preference is 24 hours. This Critical-weight item is RED because the governing vendor language falls materially short of the acceptable threshold on three independent dimensions:

1. No 72-hour hard cap. Both the QBO DPA (§ 4.4) and the Time/Workforce DPA (§ 2.9.1) use the phrase "without undue delay" with no specified maximum notification window. While "without undue delay" echoes GDPR Article 33 language — which regulators typically interpret as 72 hours — it is not a contractually enforceable ceiling. Intuit could argue that a protracted investigation before notification is permissible, eliminating the certainty that the 72-hour cap is intended to provide. The playbook's acceptable threshold explicitly requires the hard cap ("in any event within 72 hours"), and that language is absent from both DPAs.

2. Actual incidents only — suspected incidents excluded. Both DPAs trigger the notification obligation only when Intuit "becomes aware of an actual Security Incident." The playbook requires notification of "actual or suspected" breaches. Suspected-breach notification is a materially higher standard: it enables the customer to initiate its own investigation and preserve evidence at the earliest opportunity, before a breach is confirmed. Neither DPA provides this protection.

3. Scope limited to Security Incidents — general DPA breaches excluded. The "Security Incident" definition in the QBO DPA is limited to "unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Business Connection Data." The Time/Workforce DPA defines "Security Incident" as a "Personal Data Breach" under the GDPR. The playbook additionally requires notification of "any other actual or potential breach of the DPA" — for example, unauthorized sub-processing, purpose limitation violations, or cross-border transfer failures. This broader category is wholly absent from both DPAs.

Each of these three gaps independently prevents the acceptable threshold from being met. Together, for a Critical-weight item, they produce a clear RED classification. The 24-hour preference is not met. This is not a silence situation — vendor language exists but is materially weaker than required — so no silence downgrade applies. California's breach notification

statute (Cal. Civil Code § 1798.82) requires notification "in the most expedient time possible and without unreasonable delay" but does not supply a 72-hour cap, and therefore does not cure the gap.

— Superseding reasoning —
Two DPAs are relevant: the QBO Data Processing Agreement (Doc 3) governing Business Connection Data for core QuickBooks Online services, and the Time/Workforce DPA (Doc 4) governing Customer Data for QuickBooks Time, Workforce, and Contractor Payments. Both DPAs contain explicit hierarchy clauses establishing their precedence over the main Terms of Service: QBO DPA § 11.3 provides that SCCs prevail, then the DPA, then the Agreement; the Time/Workforce DPA § 4.7 likewise states the DPA controls over the Agreement for Customer Data processing. Because the main Terms of Service (Doc 1) contain no breach notification provision that could conflict with either DPA, there is no conflict to resolve between them. The two DPAs apply in parallel to their respective service scopes and use materially identical notification language ("without undue delay" for actual Security Incidents), so no superseding determination is required between them. The DPAs collectively represent the governing standard for breach notification across all QuickBooks services covered by this review.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "If Intuit becomes aware of an actual Security Incident that involves Business Connection Data, Intuit will: (a) notify Customer of the Security Incident without undue delay; (b) take appropriate steps…"
2. "If Intuit becomes aware of an actual Security Incident that involves Customer Data that Intuit is acting as a Processor of on Customer's behalf, Intuit will: (a) notify Customer of the Security Incide…"

Our liability

AI Comment: The playbook item checks that vendor (Intuit's) liability is limited to amounts paid by the customer. This item is weighted "Acceptable to Deviate," signaling low priority.

Primary Finding — GREEN: The Section A "Limitation of Liability" in the Terms of Service directly caps Intuit's aggregate liability at the greater of (1) fees paid for the relevant Service(s) in the 12 months preceding the breach, or (2) $100. This structure expressly ties Intuit's maximum exposure to amounts actually paid, satisfying the acceptable position. The provision is reinforced by a broad consequential/indirect damages exclusion and a statement that the Agreement sets out the customer's exclusive remedy. The DPA Section 10.1 defers all liability limits to the Agreement, maintaining consistency.

Service-Specific Override — YELLOW (superseded for Live Expert Services): Section B explicitly states it "will prevail over any conflict or inconsistency with the Section A Terms." For QuickBooks Live Expert Services (Live Full-Service Bookkeeping, Expert Cleanup, Full-Service Cleanup), a specific Section B liability clause overrides the Section A fee-based cap, limiting Intuit's remedy exclusively to correcting errors in QuickBooks for the month the error occurred. This removes the monetary fee-based floor and substitutes a non-monetary, specific-performance remedy. For this use case (bookkeeping/financial reporting via QuickBooks Online), customers relying on Live Bookkeeping services would have no path to fee recovery under Section B.

Superseding Determination: PIF 1 (Section B Live Expert Services Liabilities) supersedes PIF 0 (Section A General LOL) for Live Expert Services, per the explicit Section B precedence rule and the specific-over-general drafting principle. For all other QuickBooks services (core QBO, payroll, payments), the Section A fee-based cap governs.

Overall Classification: GREEN. The primary cap structure meets the acceptable position, the DPA defers consistently, and the Live Bookkeeping override—while replacing the monetary cap with specific performance—is a service-appropriate remedy for bookkeeping correction and presents low practical risk at the "Acceptable to Deviate" weight level. No preference was specified, so aiPreferenceMet is false.

— Superseding reasoning —
Section B Terms contain an explicit hierarchy clause — "These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms" — which expressly places Section B above Section A. The Section B liability clause for Live Expert Services is also more specific (scoped to a defined set of bookkeeping services) than the general Section A cap, triggering both the contractual hierarchy and the general-vs-specific drafting principle. For Live Expert Services only, the Section B clause governs; for all other Platform services, the Section A fee-based cap applies.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The total aggregate liability of Intuit and our third party providers, licensors, distributors or suppliers ("Intuit Parties") arising out of or relating to this Agreement is limited to the greater of…"
2. "The Intuit Parties won't be responsible for the following:

- Loss of data, profits, revenues, business opportunities, goodwill or anticipated savings;
- Indirect, incidental, or consequential loss;
-…"
3. "10.1Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of l…"

"Notwithstanding anything to the contrary in the Section A Terms, if any Intuit error occurs in performing the QuickBooks

> *Live Expert Services, our only responsibility will be to correct the error in QuickBooks Online for the month the error occurred."*
> — QBO Terms of Service for QuickBooks - US

Employee Access Control

AI Comment: The playbook item requires that Intuit, as a SaaS vendor processing sensitive financial and payroll data, grants system access only to authorized personnel, on a need-to-know basis, strictly limited to what is required to fulfill their function. This is a canonical principle-of-least-privilege / role-based access control requirement.

The document set partially addresses this requirement across two DPAs, but falls materially short of the explicit "strictly limited to what is required to fulfill their function" standard for the following reasons:

What the documents do address:
1. **Authorization requirement** — Both DPA 3 (QBO DPA §4.2) and DPA 4 (Time/Workforce DPA §2.4) establish that only persons *authorized by Intuit* may process customer/Business Connection Data. Unauthorized persons are expressly excluded.
2. **Confidentiality obligation** — Both DPAs require that authorized processors be bound by a duty of confidentiality (contractual, internal policy, or statutory).
3. **Purpose limitation as a proxy for need-to-know** — DPA 4 §2.4 goes further than DPA 3, adding the requirement that all Authorized Persons "Process the Customer Data only as necessary for the Permitted Purpose." This language approaches a need-to-know framing, but at the *processing behavior* level rather than as an explicit system access control commitment.
4. **General security measures** — Both DPAs commit to "appropriate technical and organisational measures" including pseudonymization, encryption, confidentiality, integrity, availability, and resilience of processing systems (DPA 3 §4.1, DPA 4 §2.5).

What the documents do NOT address:
1. **No explicit access control mechanism** — Neither DPA nor the ToS contains language specifying least-privilege, role-based access control (RBAC), access provisioning tied to job function, or access recertification. The commitment is to *behavioral* restrictions on authorized persons, not to *technical* access control systems that would prevent access being granted beyond what is required for the function.
2. **Detailed security measures deferred externally** — Both DPAs refer to the Intuit Security Center for technical and organizational security details (DPA 3 §4.1; DPA 4 §2.5). That external resource is not part of the contractual commitment and was not provided for review. This means the specific access control architecture Intuit actually implements is not contractually defined or auditable through the contract alone.
3. **DPA 3 weaker than DPA 4 on this point** — For core QuickBooks Online data (Business Connection Data), DPA 3 commits only to confidentiality obligations for authorized persons, without the "only as necessary for the Permitted Purpose" qualifier that DPA 4 provides for Workforce/Time data. QuickBooks is primarily used for bookkeeping, payroll, and financial reporting — all core QBO functionality — meaning DPA 3 governs the majority of the relevant data, with the weaker of the two formulations.

Document hierarchy note: Per DPA 3 §11.3, the order of precedence is SCCs !' DPA 3 !' ToS for QBO Business Connection Data. Per DPA 4 (How this DPA applies, bullet 3) and ToS §F.15, DPA 4 controls for Time/Workforce/Contractor Payments personal data. The two DPAs operate in parallel for their respective service scopes and do not directly conflict; no superseding determination is required between them.

Overall classification: YELLOW. The vendor addresses the general concept of authorized personnel and confidentiality through its DPA language, and DPA 4 adds a near-equivalent of "only as necessary for the Permitted Purpose." However, the acceptable position — explicit contractual commitment to system access strictly limited to what is required to fulfill each person's function, with specific access control mechanisms — is not met. The technical access control implementation is deferred to an external non-contractual resource, and the primary DPA (DPA 3 for core QBO) omits the purpose-limitation qualifier present in DPA 4. Given the High weight of this item and the sensitive nature of the data QuickBooks processes (financial records, payroll, tax data), this gap warrants documented review and assessment.

— Superseding reasoning —
Two DPAs apply across different QuickBooks service lines and do not conflict with each other — they operate in parallel scopes. DPA 3 (QBO DPA) governs Business Connection Data for core QBO services (bookkeeping, invoicing, financial reporting, payroll data) per ToS §B.7 and DPA 3 §11.3. DPA 4 (Time/Workforce DPA) governs Personal Information for Workforce, Time, and Contractor Payments services per ToS §F.15 and DPA 4 (How this DPA applies, bullet 3). Within each DPA's scope, the respective DPA supersedes the ToS where they conflict (DPA 3 §11.3: "SCCs !' this DPA !' Agreement"; DPA 4: "this DPA shall control"). No inter-document superseding is necessary because the DPAs address non-overlapping service lines.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall ensure that any person that it authorizes to Process the Customer Data (including Intuit's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of …"

> *"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymisation or encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

For more information about our technical and organizational measures to protect the Data from a Security Incident please see: https://security.intuit.com/security-practices"
— QuickBooks Time & Workforce (Time/Payroll) DPA
"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."
— Global Privacy Statement | Intuit

Publicity

AI Comment: The documents do not contain an explicit "Publicity" or "Reference" clause governing Intuit's right to use the customer's name, logo, or trademark in marketing materials, customer lists, press releases, or case studies. The absence of an affirmative marketing-use grant is partially favorable — Intuit has not been explicitly authorized to use our logo for publicity. However, the acceptable position requires that prior consent be obtained before any marketing use of our logo, and the ideal preference requires an explicit prior-written-consent mechanism. Neither requirement is affirmatively established by any document in the set.

The nearest directly relevant provision is the broad Content license in the ToS "Content and Data" section. "Content" is defined to include "data, information, materials, text, graphics, images, audio, video that are uploaded, transmitted, posted, generated, stored, or otherwise made available through the Platform" — a scope wide enough to capture customer logos (e.g., a company logo uploaded for use on QuickBooks-generated invoices). The license grants Intuit the right to "publish or publicly display," "reproduce," "distribute," and create "derivative works" of such Content. The purpose limitation — restricted to "operating, providing and improving the Platform" — provides partial protection that broadly aligns with the preference's acceptable service-provision carve-out. However, "improving the Platform" is ambiguous and could be stretched to encompass product demonstrations or promotional use. There is no explicit prohibition on marketing use of the customer's logo.

The Content license duration extends "for as long as your Content is protected by intellectual property rights." For a trademark-protected logo (trademark rights do not expire when actively maintained), this creates a potentially perpetual license — one that survives the subscription period and does not terminate upon contract expiration.

The feedback license ("Community Forums; Feedback" section) is separately notable: it explicitly includes "advertising or marketing materials" within its scope, though it applies specifically to "feedback, suggestions, and ideas" rather than standalone logo or trademark use. If branded materials appear within customer feedback, this provision creates an additional, broader exposure.

Neither the Terms of Service, the Global Privacy Statement, nor either DPA contains an explicit requirement that Intuit obtain prior written consent before using the customer's name or logo for marketing, nor an explicit prohibition on such use. The acceptable position (consent required for marketing logo use) and the ideal preference (explicit prior-written-consent requirement with a narrow service-provision carve-out) are both unmet. Classification is YELLOW: the subject is partially addressed through the purpose-limited Content license, but the explicit protective mechanism the playbook requires is absent, and the broad scope of "Content" combined with an ambiguous purpose clause and perpetual duration creates interpretive risk for the customer.

"Content includes, but is not limited to, data, information, materials, text, graphics, images, audio, video that are uploaded, transmitted, posted, generated, stored, or otherwise made available through the Platform."
— QBO Terms of Service for QuickBooks - US
"Content and Data"
— QBO Terms of Service for QuickBooks - US
"Duration

This license lasts for as long as your Content is protected by intellectual property rights."
— QBO Terms of Service for QuickBooks - US

"You grant Intuit a perpetual, worldwide, fully transferable, sub-licensable, irrevocable, fully paid-up, royalty free license to use your feedback, suggestions, and ideas in any way, including in future modifications of the Platform, other products or services, advertising or marketing materials."
— QBO Terms of Service for QuickBooks - US

Physical Security Controls

AI Comment: The document set partially addresses physical security controls but does so in vague, high-level terms that are insufficient to confirm the vendor meets this High-weight requirement. The strongest reference is a single sentence in the Global Privacy Statement asserting "reasonable physical, technical and organizational safeguards" — but this statement is contained in a unilaterally amendable privacy notice, not a binding contractual commitment, and it describes no specific controls, policies, or access mechanisms. Both the QBO DPA (§4.1) and the Time/Workforce DPA (§2.5) make enforceable security commitments, but the measures they enumerate — pseudonymization/encryption, availability/resilience, restore capability, and effectiveness testing — are technical and organizational in nature; physical security controls are conspicuously absent from those enumerations. The QBO DPA's §5 commitment to make security audit reports (at intuit.com/compliance/) available provides indirect assurance that physical controls are certified externally (e.g., SOC 2 Type II typically covers physical access), but those reports are external to the contract and not provided in this document set. For a High-weight item requiring affirmative evidence that the vendor has documented system controls and policies to prevent unauthorized physical access, the contract language falls short of the acceptable position. Classification is YELLOW: the topic is not entirely silent, but the coverage is too general and non-specific to confirm compliance. The reviewing attorney should request Intuit's current SOC 2 Type II or equivalent audit report to assess whether physical access controls are adequately described and independently certified.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"

"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information."
— Global Privacy Statement | Intuit
"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymisation or encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."
— QuickBooks Time & Workforce (Time/Payroll) DPA

Insurance

AI Comment: All six documents in the review set — the QuickBooks Terms of Service (Section A Platform Terms and Section B Product Specific Terms), the Global Privacy Statement, the QuickBooks Online Data Processing Agreement, the QuickBooks Time & Workforce DPA, the Intuit Telecom Specific Terms, and the Acceptable Use Policy — are entirely silent on Intuit's obligation to maintain any form of insurance coverage. There is no mention of general liability, professional liability/E&O, technology/cyber liability, workers' compensation, or any other insurance maintained by Intuit as vendor. The only insurance references appearing in the documents concern employee benefit plan insurance offered by Intuit to its customers' employees (e.g., health insurance, worker's compensation as Third-Party Partner Plans under Part F Section 9d of the ToS), and a disclaimer that Intuit is not itself an insurance carrier — neither of which addresses vendor insurance coverage. The contract is completely silent on this playbook requirement.

Silence-handling framework applied:

1. **Silence confirmed:** No relevant language exists across any document in the set.
2. **Item weight is "Acceptable to Deviate":** Default silence classification is YELLOW.
3. **Industry norm evaluation:** It is universal SaaS industry practice for public-facing Terms of Service to not include the vendor's own insurance obligations. Such requirements — when commercially required — are addressed through separately negotiated Master Service Agreements, vendor questionnaires, insurance certificates, SOC 2 audit reports, or bespoke addenda, not in standard click-wrap ToS. The absence of insurance language in public SaaS ToS is the market norm across all major SaaS providers, not a meaningful gap specific to Intuit.

4. **Practical risk:** Intuit is a large, publicly traded enterprise (NASDAQ: INTU) that processes sensitive financial data — payroll, bookkeeping, tax — for millions of customers globally. Companies of this scale and regulatory exposure universally maintain substantial insurance portfolios (general liability, professional liability/E&O, cyber/technology liability, D&O) as a matter of business necessity, investor expectations, and lender covenants. The practical risk of Intuit operating without insurance is extremely low, even though no contractual commitment is made in the ToS.
5. **Downgrade applied:** YELLOW !' GREEN, one level, on INDUSTRY_NORM basis.

The item weight of "Acceptable to Deviate" independently reinforces the GREEN outcome — the reviewing organization has pre-determined this is a low-priority concern.

Reviewer note: If a contractual insurance commitment is required (e.g., to satisfy the organization's internal vendor risk policy, as a backstop for indemnification claims, or to comply with procurement thresholds), this must be raised through Intuit's enterprise sales or legal channel and negotiated as a bespoke addendum. It will not be obtained via the standard public ToS. Confidence is MODERATE because the GREEN determination rests on industry-norm reasoning rather than explicit contractual text.

— Applied silence standard —
Basis: INDUSTRY_NORM
Citation: Public-facing SaaS vendor Terms of Service universally do not address the vendor's own insurance obligations. Insurance commitments, when commercially required, are captured in separately negotiated MSAs, vendor questionnaires, insurance certificates, or SOC 2 reports — not in standard click-wrap ToS. For a large, publicly traded SaaS provider of Intuit's scale (NASDAQ: INTU), the practical risk of the vendor operating uninsured is extremely low given market and regulatory expectations on companies of this size.

Data Protection Officer (DPO)

AI Comment: The acceptable position requires Intuit to have designated a Data Protection Officer ("DPO") or a named privacy point of contact with sufficient qualifications. The Global Privacy Statement — expressly incorporated into the QuickBooks Terms of Service by reference and therefore contractually binding — explicitly uses the formal title "Data Protection Officer" and provides a contact mechanism (web submission form) for that role across three distinct jurisdictional sections: United States, Canada, and United Kingdom/EEA/Switzerland. This satisfies the acceptable threshold: a DPO has been formally designated and is reachable.

For the ideal preference — a demonstrably "qualified" DPO — the documents fall short. The DPO is not identified as a named individual; no specific professional qualifications, certifications, or expert credentials are stated anywhere in the document set; and contact is limited to a generic web form rather than direct DPO contact details (e.g., a dedicated email or phone). In the governing jurisdiction (California, US), neither the CCPA nor other applicable California law imposes a formal DPO designation requirement with specific qualification standards (as GDPR Articles 37–39 would in EU/UK contexts). While the GDPR-context reference in the UK/EEA section implies the role is held by someone meeting at least those qualifications for that regulatory regime, that inference cannot be reliably extended to the US governing context. Accordingly, the "qualified" element of the ideal preference is not independently verifiable from the available documents.

Classification: GREEN. The acceptable threshold is clearly met by formal DPO designation with contact information across multiple jurisdictional sections of the incorporated Global Privacy Statement. aiPreferenceMet is false because the qualification standard required by the ideal preference is not demonstrated in the documents.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit Inc.

Attention: Privacy

2800 E Commerce Center Place

Tucson, AZ 85706

You can contact the Intuit Data Protection Officer here."

> *"United Kingdom, EEA and Switzerland contact information:**"*
> — Global Privacy Statement | Intuit
> *"Canada contact information:**"*
> — Global Privacy Statement | Intuit

Termination for Convenience

AI Comment: The playbook's acceptable position has three discrete requirements: (1) the customer may terminate for convenience; (2) the vendor may not terminate for convenience; (3) either party's termination for convenience entitles the customer to a pro rata refund of remaining unused fees.

Element 1 — Customer can terminate for convenience: MET. The Terms of Service confirm the customer may cancel at any time (§ "Payment & Cancellations"). Upon mid-period cancellation the customer retains access through the end of the current subscription period. This element is satisfied.

Element 2 — Vendor cannot terminate for convenience: NOT MET (direct conflict). Section A "Termination" expressly

grants Intuit an unrestricted, unilateral right to terminate "at any time in our discretion," with no stated basis, no notice requirement, and no qualifying condition. This is a textbook termination-for-convenience right and directly contradicts the acceptable position. A limited improvement exists for QuickBooks Money specifically (Section B Part X), where Intuit must provide 15 days' prior notice before terminating for any reason — but the convenience right itself is preserved even there. Per the explicit Section B precedence clause, the QB Money provision supersedes Section A for that sub-product. However, the core QBO product (the primary service per the intake brief: bookkeeping, payroll, and financial reporting) remains governed by the unrestricted Section A language.

Element 3 — Pro rata refund upon termination: NOT MET (direct conflict). Section A "Payment & Cancellations" states categorically that Intuit does "not provide refunds or credits for any cancellations or partial subscription period." Section A "Effect of Termination" reinforces this: no termination, by either party, entitles the customer to any refund. This no-refund position is reiterated in each product-specific Section B tier reviewed (QuickBooks Live Priority, Live Expert Assisted, Full-Service Bookkeeping, Expert Cleanup / Full-Service Cleanup, and IAS). Critically, the no-refund provision applies even when Intuit initiates termination — meaning the customer could lose the entirety of a prepaid annual subscription with no recourse if Intuit exercises its Section A termination right.

Overall classification: RED. Two of three requirements of the acceptable position are explicitly contradicted by vendor terms. Given the item weight is "Acceptable to Deviate," the risk matrix places this in the "Noted — comment recommended" tier. The practical exposure worth flagging for the reviewing lawyer is the asymmetry on Intuit-initiated termination: customers on prepaid annual subscriptions face the risk of total fee forfeiture with no notice and no refund if Intuit invokes its Section A termination right.

— Superseding reasoning —
The opening of Section B (Product Specific Terms) contains an explicit document-hierarchy clause: "These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms." For QuickBooks Money specifically (Part X), the termination provision requires 15 days' prior notice before Intuit terminates for any reason — a more customer-favorable condition than the Section A "at any time in our discretion" right. Accordingly, the QB Money Section B provision supersedes the Section A provision for that sub-product. However, the core QBO product (primary use case per the intake brief) is not covered by the QB Money-specific Part X terms; Section A's unrestricted termination right continues to govern QBO directly. The governing language for the primary product remains the Section A clause.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit further reserves the right to terminate this Agreement with respect to QuickBooks Money at its sole discretion and for any reason with fifteen (15) days' prior notice."

> *"Your payment to Intuit will automatically renew at the end of the applicable subscription period but you can cancel a subscription at any time."*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit may terminate this Agreement (and your account) or suspend the Platform at any time in our discretion."*
> — QBO Terms of Service for QuickBooks - US
> *"We do not provide refunds or credits for any cancellations or partial subscription period."*
> — QBO Terms of Service for QuickBooks - US
> *"No expiration or termination will affect your obligation to pay all fees due or that may have accrued through the effective date of expiration or termination or entitle you to any refund."*
> — QBO Terms of Service for QuickBooks - US

Data Ownership

AI Comment: The playbook item requires that, as between the parties, all Personal Data remains the sole property of the customer's company. This Critical-weight item is not met. The Intuit/QuickBooks document suite directly and explicitly conflicts with this standard across multiple provisions, and even the most favorable governing language (the DPA framework) fails to satisfy "sole property."

Primary conflicts:

1. **Intuit claims outright ownership of de-identified/aggregated data derived from customer Personal Data** (ToS §Content and Data): "Intuit will own all such data and may use this data without restriction." This is a direct property claim over data originating as the customer's personal data, exercisable for marketing and product improvement without limitation. The QBO DPA permits de-identification but is silent on ownership of the resulting data, leaving the ToS ownership claim operative.

2. **Intuit acts as an independent data controller for commercial purposes even under the DPA** (QBO DPA §2.1): The DPA's processor appointment is immediately qualified — Intuit remains a controller when using Business Connection Data for product development, data analytics, fraud prevention, and marketing. A controller independently determines the purposes and means of processing, which is structurally incompatible with the customer having "sole property" rights over that data. This is not a minor carve-out: it encompasses Intuit's core commercial data activities.

3. **Global Privacy Statement confirms Intuit's independent controller status**: Intuit "determines the purposes and means of the processing of your personal information...and therefore acts as a 'data controller.'" This is a parallel and consistent confirmation that Intuit exercises independent data rights — not solely as a processor on the customer's behalf.

4. **Cross-platform data sharing for Intuit's commercial benefit** (ToS §Agreement to These Terms): By accepting the Terms, the customer expressly "instruct[s]" Intuit to share data across the Intuit Platform for marketing and eligibility

purposes. The companion provision in §Your Personal Information confirms that intra-Intuit Group sharing "is contemplated as part of the Platform." These provisions establish Intuit's commercial data rights as a feature of the service, not a deviation from it.

5. **Workforce Services broad data license** (ToS Part F §15): A worldwide, royalty-free license to collect, use, modify, create derivative works from, and use Personal Information to "improve…other Intuit products" — well beyond processing on the customer's behalf. While this is superseded by the Time/Workforce DPA for Customer Data processing, the Time/Workforce DPA itself designates Intuit as Controller of Account Data (defined broadly to include account-related, feedback, training, and event data), further fracturing any "sole property" claim.

What partially supports the standard (insufficient):
- The ToS states "Your Content remains yours" preserving customer IP rights, and the DPA (which supersedes the ToS for Business Connection Data per DPA §11.3) establishes a processor appointment for most Business Connection Data processing. These elements are real but insufficient: (a) the content IP retention is immediately qualified by a perpetual broad license including sublicensing and derivative works rights; (b) the DPA's own controller carve-out negates sole property for the most commercially significant uses; and (c) de-identified/aggregated derivatives are owned by Intuit under the ToS without DPA reassignment to the customer.

After superseding: The QBO DPA §2.1 governs over the ToS's general Content and Data provisions for Business Connection Data (per DPA §11.3). The Time/Workforce DPA §2.1 governs over the ToS's Workforce Data Rights (per ToS §F §15 cross-reference and Time/Workforce DPA hierarchy clause). Even under these governing DPA provisions, Intuit's controller role for commercial purposes, ownership of de-identified derivatives, and controller status over Account Data remain operative conflicts. Classification: RED — the vendor terms explicitly establish data rights in Intuit that are irreconcilable with "sole property of our company."

— Superseding reasoning —
Two cross-document superseding determinations apply. First, for Business Connection Data: QBO DPA §11.3 establishes an explicit precedence order — SCCs, then DPA, then Agreement — meaning the QBO DPA §2.1 processor/controller framework governs over the ToS's general Section A Content and Data provisions. The Section B Terms in the ToS itself also provide that Section B prevails over Section A, and Section B §7 points to the DPA for processing roles, reinforcing this hierarchy. Second, for Workforce/Time Customer Data: ToS Part F §15 contains an internal cross-reference stating the Time/Workforce DPA controls over any Agreement discrepancy "with respect to the collection, use, and/or disclosure of Personal Information," and the Time/Workforce DPA's own applicability clause independently states the DPA controls over the Agreement for Customer Data processing. These superseding determinations do not resolve the RED classification, because (a) the governing QBO DPA §2.1 itself preserves Intuit's controller role for product development, data analytics, and marketing; (b) the governing Time/Workforce DPA §2.1 designates Intuit as Controller of Account Data; and (c) the ToS's de-identified/aggregated data ownership claim (§Content and Data) is not addressed — let alone reassigned to the customer — by either DPA.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit may collect, derive or generate deidentified and/or aggregated data regarding your usage of or the performance of the Platform, including data derived from your Content. Intuit will own all suc…"
2. "By using the Platform, you are instructing us to share your data across our Platform for marketing, eligibility, and other purposes described in our Global Privacy Statement, consistent with applicabl…"
3. "In your use of the Workforce Services you are hereby granting Intuit a non-exclusive, worldwide, royalty-free right and license to collect, use, copy, display, perform, store, transmit, modify and cre…"
4. "Customer (in its role as Controller) appoints Intuit as a Processor to Process the Customer Data when Intuit is acting directly on Customer's behalf. Intuit shall be the Controller of Account Data and…"

> *"Your Content remains yours, which means that you retain any intellectual property rights that you have in your Content. By sharing your Content on the Platform, you hereby grant Intuit a license to use your Content, as described in more detail below."*
> — QBO Terms of Service for QuickBooks - US
> *"For the purposes of Intuit providing Services to Customer, Customer (whether itself a controller or a processor on behalf of a third-party controller) appoints Intuit as a processor to process Business Connection Data. Provided, however, that the parties acknowledge that Intuit shall be a controller when Intuit uses Business Connection Data for certain limited purposes, as further described in the Agreement (including, for example, in relation to Intuit product development and improvement, data analytics, and fraud prevention and security), for product and service improvement, and to market Intuit's products and services."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Scope of this Privacy Statement and our role"*
> — Global Privacy Statement | Intuit

User Authentication Policies

AI Comment: The playbook item requires that the vendor have documented policies for user authentication and password protection. The document set confirms that Intuit does maintain such policies, addressing the item's acceptable threshold.

Authentication Policies — Present: Intuit explicitly describes MFA (multi-factor authentication) via SMS security codes as a deployed authentication control, appearing in at least three separate documents: the Section A Terms (Intuit Communications), the Section B Terms (Part 4 – Telephone Numbers), and the Intuit Telecom Specific Terms. The ToS also acknowledges single sign-on (SSO) integration as an alternative authentication pathway, with a notable caveat that third-party SSO services "may not have the same authentication and security features as the Services," suggesting Intuit's own authentication posture is the baseline.

Password Protection Policies — Present: The ToS requires users to "securely manag[e]" their account credentials, including user IDs and passwords, and mandates immediate notification in the event of compromise. The QuickBooks Payments section contains more specific obligations: users receiving platform access credentials must keep them confidential, not share them, and be responsible for all actions taken under those credentials.

Technical Security Measures — Present in DPAs: Both the QBO DPA and the Time/Workforce DPA obligate Intuit to implement "appropriate technical and organisational measures" that include pseudonymization/encryption, confidentiality/integrity/availability controls, and periodic testing of security effectiveness. While these measures are described at a general level rather than authentication-specifically, they underpin the authentication policy framework.

Classification Rationale — GREEN with caveats: The acceptable position is met: the vendor has documented authentication and password protection policies. However, several gaps prevent an ideal/preference-met classification: (1) MFA is described with permissive "may use" language rather than as a mandatory universal control; (2) no password complexity or rotation requirements are stated in the agreement documents; (3) no account lockout or brute-force protection policies are described; (4) session management policies are absent; and (5) detailed authentication standards are deferred to the Intuit Security Center (security.intuit.com) rather than incorporated into the agreement. The classification is GREEN but with MODERATE confidence given the gap between what the documents contain versus comprehensive authentication policy coverage expected for a SaaS platform processing payroll and financial data.

— Superseding reasoning —
Multiple documents address authentication and password protection without conflict — they are additive and consistent. The Section B Terms explicitly prevail over Section A Terms on any conflict (ToS, Section B preamble), and the QBO DPA prevails over the Agreement per Section 11.3 (SCCs > DPA > Agreement). Because the authentication and password protection provisions across documents are consistent rather than conflicting, no superseding determination alters any classification. The Section B Part 4 Telephone Numbers language on MFA is more detailed than the Section A language but does not contradict it; it is appropriately treated as the more specific and controlling statement of MFA policy for QuickBooks Online services.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "You understand and agree that Intuit may use your telephone number for multi-factor authentication ("MFA"), to confirm your identity and help protect the security of your account. Part of the MFA iden…"
2. "If you receive a user identification name or password from us to access our database or use QuickBooks Payments (the "Account Access Password"), you will: (a) keep the Account Access Password confiden…"

> *"You are responsible for securely managing your Account Information, including your user ID and any password(s) for the Platform. You will notify us immediately if you believe your Account Information or device you use to access the Platform has been lost or stolen or that someone is using your account without your permission."*
> — QBO Terms of Service for QuickBooks - US
> *"You understand and agree that Intuit may use your telephone number for "multi-factor authentication" ("MFA"), to confirm your identity and help protect the security of your account. Part of the MFA identity verification process may involve Intuit sending text messages containing security codes to your telephone number. You agree to receive these texts from Intuit containing security codes as part of the MFA process. In addition, you agree that Intuit may send automated text messages and pre-recorded voice messages to the telephone number you provide for other limited purposes, including: providing you with important critical notices regarding your use of the Services, or fulfilling a request made by you through the Services."*
> — QBO Terms of Service for QuickBooks - US
> *"Certain Services on the Platform enable single sign-on integration. By enabling single sign-on, you are authorizing access and use of certain Services directly from a third-party service. Such third-party service may not have the same authentication and security features as the Services. You assume all risk and responsibility arising from the use of, and access to and from, the Services enabled through single sign-on."*
> — QBO Terms of Service for QuickBooks - US
> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."
— QuickBooks Time & Workforce (Time/Payroll) DPA
"You understand and agree that Intuit may use your telephone number for "multi-factor authentication" ("MFA"), to confirm your identity and help protect the security of your account. Part of the MFA identity verification process may involve Intuit sending text messages containing security codes to your telephone number. You agree to receive these texts from Intuit containing security codes as part of the MFA process."
— Intuit Telecom Specific Terms
"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."
— Global Privacy Statement | Intuit

Retention of our Rights to our Property

AI Comment: The Review Specific Playbook item requires that transfer of ownership of the customer's products, services, materials, content, or data to the vendor be prohibited. The document set directly addresses this topic across the Terms of Service and the QuickBooks Online Data Processing Agreement, but the combined provisions produce a mixed picture that falls short of the acceptable position.

What is GREEN: The ToS explicitly states "Your Content remains yours, which means that you retain any intellectual property rights that you have in your Content" (Section A, "Content and Data"). This is a direct, unambiguous acknowledgment of customer IP retention and, standing alone, would support a GREEN finding.

What undermines the GREEN: Three provisions materially weaken the customer's ownership protection:

1. **Deidentified/aggregated data ownership (RED concern):** The ToS grants Intuit the right to "collect, derive or generate deidentified and/or aggregated data regarding your usage of or the performance of the Platform, including data derived from your Content," and then explicitly states that "Intuit will own all such data and may use this data without restriction." This is an unqualified claim of Intuit ownership over data derived from the customer's content — a direct transfer of an ownership interest in the informational value of customer data. For QuickBooks' intended use case (bookkeeping, income/expense tracking, payroll, financial reports), the financial patterns and business insights that can be derived from raw customer data are themselves commercially sensitive and valuable. The QuickBooks Online DPA's Annex B (United States) corroborates this, expressly permitting Intuit to "de-identify or aggregate Business Connection Data as part of performing the Service." This provision conflicts with the playbook's prohibition on ownership transfer and is the primary driver of the YELLOW classification.

2. **Broad, effectively perpetual license (YELLOW concern):** Intuit obtains a worldwide, non-exclusive, royalty-free, sublicensable license to host, reproduce, distribute, communicate, sublicense, use, modify, and create derivative works from customer content. This license endures "for as long as your Content is protected by intellectual property rights" — effectively in perpetuity for most business content protected by copyright. The "Content and Data" Survival clause in Section A further confirms these license rights survive termination of the agreement. While technically a license (not an ownership transfer of raw content), the scope — particularly sublicensing and derivative works rights — approaches ownership-like interests over the customer's data in practical effect. The license purpose is stated as limited to "Operating, providing and improving the Platform," but the deidentified-data clause separately grants unrestricted use of derived data for all purposes including marketing, which functionally circumvents that limitation.

3. **Assignment without notice (YELLOW concern):** Intuit may "assign or transfer this Agreement to any party at any time without notice to you." Because the Agreement includes the broad license over customer content, this provision allows Intuit to place all of its content rights — including sublicensing rights over customer's data — into the hands of an unknown third party without customer knowledge or consent. This directly conflicts with the playbook's objective of prohibiting ownership/control transfer regarding the customer's property.

Superseding framework: The DPA prevails over the Agreement in case of conflict (DPA §11.3). The DPA's deidentification provision (Annex B, US §07) is consistent with — and reinforces rather than limits — the ToS's deidentified data ownership claim. Section B Terms prevail over Section A Terms per Section B's introductory language; no Section B QuickBooks-specific provision meaningfully overrides or limits the Section A content ownership analysis.

Summary: The explicit "Your Content remains yours" language prevents a RED classification, but the explicit Intuit ownership claim over derived/aggregated data, the perpetual and sublicensable license, and the unconsented assignment right collectively mean the vendor terms do not fully satisfy the playbook's requirement that ownership transfer be prohibited. This is a YELLOW finding on a Critical-weight item requiring documented review and assessment.

— Superseding reasoning —

The DPA prevails over the Agreement in case of conflict per DPA Section 11.3. However, the relevant provisions across the ToS and DPA are consistent and mutually reinforcing rather than in conflict: both documents permit Intuit to deidentify/aggregate customer data (ToS §Content and Data; DPA Annex B US §07). Section B Terms prevail over Section A Terms per Section B's introductory clause, but no Section B QuickBooks-specific provision directly overrides the Section A content/data ownership provisions. No superseding determination is required because the documents are aligned on the key provisions, not in conflict.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "This license is:

Worldwide, which means it's valid anywhere in the world;

Non-exclusive, which means you can license your Content to others; and

Royalty-free, which means there are no fees for this…"
2. "Intuit may collect, derive or generate deidentified and/or aggregated data regarding your usage of or the performance of the Platform, including data derived from your Content. Intuit will own all suc…"

> *"Your Content remains yours, which means that you retain any intellectual property rights that you have in your Content."*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit may assign or transfer this Agreement to any party at any time without notice to you."*
> — QBO Terms of Service for QuickBooks - US
> *"Notwithstanding any use restriction contained elsewhere in this Annex B, Intuit may de-identify or aggregate Business Connection Data as part of performing the Service specified in this DPA and the Agreement."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"For the purposes of applicable data protection laws, you agree and acknowledge that there are instances in which we process Business Connection Data as a data controller for certain limited purposes, including for example, in relation to our product development and improvement, data analytics, and fraud prevention and security. In those cases, the terms of our Global Privacy Statement govern our processing of Business Connection Data."*
> — QBO Terms of Service for QuickBooks - US

Governing Law

AI Comment: The governing law is California (plus the Federal Arbitration Act for dispute resolution), as stated explicitly in the Terms of Service Section A "Governing Law." California is not one of the enumerated jurisdictions in the playbook item (Michigan, Delaware, New York), but the playbook's acceptable position expressly allows for "another jurisdiction with a reasonable connection (nexus) to either party — e.g., where a party is incorporated or headquartered." California satisfies this criterion directly: Intuit Inc. is headquartered at 2700 Coast Avenue, Mountain View, CA 94043 (confirmed across multiple document sections), making California its principal place of business. This is precisely the type of nexus the playbook contemplates. The QBO DPA reinforces this by expressly deferring its own governing law to the Agreement's governing law provisions. Notably, the TOS also confirms Intuit is incorporated in Delaware (an explicitly listed playbook jurisdiction), though the parties chose California as the governing law rather than the state of incorporation — a common and commercially reasonable choice when a vendor's operational headquarters differ from its state of incorporation. Given the weight of "Acceptable to Deviate" and California's clear, undisputed nexus to Intuit as its principal place of business, this classification is GREEN with HIGH confidence.

— Superseding reasoning —
The QBO DPA (Document 3, §11.6) contains a governing law clause that defers entirely to the Agreement's governing law provisions, rather than establishing an independent governing law. This means the TOS governing law clause (Document 1, Section A "Governing Law") is the sole operative provision on this topic. The DPA clause is superseded by the TOS clause under a document hierarchy rationale: the DPA itself directs that the Agreement controls governing law. The final controlling text is California law from the TOS.

> *"California law and the Federal Arbitration Act will govern all disputes arising out of or relating to the Platform, this Agreement and any Additional Terms, regardless of conflict of laws rules."*
> — QBO Terms of Service for QuickBooks - US
> *"This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Data Subject Rights Assistance

AI Comment: The playbook requires two distinct obligations: (1) the vendor must **first notify** the customer upon receipt of a data subject rights (DSR) request, and (2) the vendor must **promptly assist** the customer in fulfilling that request. Both the QBO Data Processing Agreement (Doc 3, §8.1) and the QuickBooks Workforce & Time DPA (Doc 4, §2.7) address these obligations, but each falls short of the unqualified standard the playbook requires, resulting in a YELLOW classification.

Notification obligation — partial alignment:
Under the QBO DPA §8.1, Intuit commits to "promptly notify Customer" only when Intuit is already "required to respond" to a DSR, and further only "where the Customer is identified or identifiable from the request." This is conditional notification: Intuit can receive a DSR, redirect the data subject to the Customer (without a formal notification to the customer organization), and never trigger the "promptly notify" obligation if it determines it is not required to respond. The playbook's "first notify us of rights request" contemplates proactive, unconditional notification upon receipt — not a conditional

notification triggered only when Intuit is about to respond. The Workforce & Time DPA §2.7.2 does not include an explicit notification-to-customer-upon-receipt commitment; instead, it directs the data subject back to Customer and provides assistance on request. Neither DPA definitively closes the gap of proactively notifying the customer organization upon mere receipt of every DSR directed to Intuit.

Assistance obligation — qualified alignment:
Both DPAs commit to assistance but with meaningful qualifiers: the QBO DPA commits to "reasonable assistance…to the extent possible" (§8.1), while the Workforce/Time DPA commits to "commercially reasonable assistance as Customer may reasonably request" (§2.7.2). These are weaker than the playbook's unqualified "promptly assist" standard, particularly since "to the extent possible" introduces a further limiting condition.

Controller carve-out — significant gap:
Section 8.1 of the QBO DPA expressly states: "nothing in the Agreement (including this DPA) shall restrict or prevent Intuit from responding to any data subject or data protection authority requests in relation to personal data for which Intuit is a controller." Intuit explicitly acts as a controller for certain purposes — including product development, data analytics, and fraud prevention (QBO DPA §2.1; Global Privacy Statement). For DSRs directed at data Intuit processes in its controller capacity, neither notification nor assistance obligations under the DPAs apply.

Scope note: The two DPAs are complementary, not conflicting — the QBO DPA governs Business Connection Data in the core accounting product; the Workforce/Time DPA governs Customer Data in the Workforce, Time, and Contractor Payments services. Both are relevant to the overall QuickBooks deployment described in the intake brief. Both DPAs prevail over the Terms of Service for data processing matters per their respective hierarchy clauses (QBO DPA §11.3; Workforce/Time DPA §4.7).

Overall: The core obligations are present in the DPAs, preventing a RED classification. However, the conditional nature of the notification trigger, the "reasonable assistance…to the extent possible" qualification on the assistance obligation, and the controller-data carve-out collectively prevent GREEN. For a High-weight item, these gaps require documented assessment before acceptance.

— Superseding reasoning —
The QBO DPA (Doc 3) and the Workforce & Time DPA (Doc 4) govern different data types and service lines within the QuickBooks platform — they are complementary rather than conflicting for this playbook item. Both DPAs prevail over the Terms of Service for data processing matters per their respective hierarchy clauses (QBO DPA §11.3 establishes SCCs !' DPA !' Agreement precedence; Workforce/Time DPA §4.7 states the DPA controls discrepancies with the Agreement regarding Customer Data processing). No intra-item superseding determination is required between the two DPAs as they address non-overlapping scopes.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall, considering the nature of the processing, provide reasonable assistance to Customer to the extent possible to enable Customer (or its third-party controller) to comply with its data prot…"
2. "So long as the Agreement is in effect, Intuit shall, in a manner consistent with the functionality of the Services and taking into account the nature of the Processing, provide reasonable assistance t…"

Processing Location Restrictions

AI Comment: The playbook acceptable position requires that all processing by Intuit occurs within the US, Canada, or EU, OR that processing outside those jurisdictions is governed by Standard Contractual Clauses (SCCs). The document set addresses this topic across three instruments — the QBO Terms of Service, the QBO Data Processing Agreement (DPA), and the Time/Workforce DPA — but the coverage is tiered by data category, with a material gap for the primary data type relevant to this California-governed QuickBooks bookkeeping deployment.

Primary data category gap (general US Business Connection Data): The QBO DPA §6.1 — the controlling instrument for Business Connection Data per the DPA precedence clause (§11.3) — explicitly permits worldwide processing: "anywhere else in the world where Intuit, Intuit Group entities or its Sub-processors maintain data processing operations." This provision contains no geographic restriction to US/Canada/EU, and the DPA does not mandate SCCs for non-EEA transfer destinations for US-originating data. The compliance-with-applicable-law qualifier ("in compliance with the requirements of Data Protection Laws") does not substitute for an SCC commitment: US law (including California's CCPA) does not require SCCs for outbound data transfers the way GDPR does. This fails both legs of the playbook acceptable position for general bookkeeping, financial reporting, and income/expense tracking data — the core categories used in this deployment.

EEA/UK/Swiss data (partial satisfaction): QBO DPA §6.3 requires use of the Data Privacy Framework for US-bound transfers of EEA/UK/Swiss Business Connection Data and mandates incorporation of SCCs where DPF is unavailable or invalidated. The Time/Workforce DPA §2.3 further requires consent, adequacy decisions, or SCCs before EEA Customer Data is transferred outside the EEA under those services. These provisions satisfy the SCC alternative for EU-originating data. However, this review's governing jurisdiction is California, US — EU data protections do not extend to the US customer's general data.

Payroll Services data (satisfies location requirement): QBO DPA §6.4 imposes an absolute US-only restriction ("no Payroll Services data will be transferred out of the United States"), exceeding the playbook's geographic requirement for that category.

Global Privacy Statement: The Privacy Statement similarly allows worldwide processing ("in any other country") and references "appropriate safeguards" for cross-border transfers, but this language is superseded by the DPA for Business Connection Data and is in any event too vague to constitute a binding SCC commitment.

Net assessment: The playbook requirement is met for EU-originating data (SCC alternative satisfied) and for payroll data (location restriction satisfied). However, for the primary data category in this review — general US customer financial and bookkeeping data processed under QuickBooks Online — the QBO DPA's worldwide processing permission, without a corresponding SCC mandate for non-EEA destinations, does not satisfy either leg of the acceptable position. Given this is a HIGH weight item, the gap warrants documented assessment and senior legal attention. Classification is YELLOW rather than RED because significant data categories do satisfy the acceptable position and the topic is substantively addressed across the document set.

— Superseding reasoning —
The QBO DPA (Doc 3) establishes its own explicit precedence hierarchy over the Agreement — which incorporates the Global Privacy Statement — per §11.3: "In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement." The DPA therefore controls over the Privacy Statement for Business Connection Data processing and transfer matters. Within the QBO DPA, the specific geographic restrictions in §6.3 (EEA/UK/Swiss SCCs and DPF) and the payroll prohibition in §6.4 override the general worldwide transfer permission in §6.1 under the specific-over-general canon for those respective data categories. The Time/Workforce DPA (Doc 4) is the controlling instrument for Customer Data processed under Time, Workforce, and Contractor Payments services — its applicability clause states it controls over the Agreement for Customer Data discrepancies — and provides more stringent EEA transfer controls than the QBO DPA §6.1 for those services. No competing hierarchy clause conflict between the two DPAs requires escalation for human resolution; they govern different service categories without contradiction.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall not transfer the Customer Data outside of the European Economic Area ("EEA") unless (a) it has first obtained Customer's prior written consent; or (b) either (i) such transfer of Customer…"

> *"Customer acknowledges that Intuit may transfer and process Business Connection Data to and in the United States and anywhere else in the world where Intuit, Intuit Group entities or its Sub-processors maintain data processing operations. Intuit shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"If GDPR requires that appropriate safeguards are put in place (for example, if the Data Privacy Framework does not cover the transfer to Intuit and/or the Data Privacy Framework is invalidated) the SCCs shall be incorporated into and form an integral part of this DPA."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"For clarity, no Payroll Services data will be transferred out of the United States."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Intuit reserves the right to store and process your personal information in the United States and in any other country where Intuit or its affiliates, subsidiaries, or service providers operate facilities in accordance with and as permitted by applicable laws and regulations. Some of these countries may have data protection laws that are different from the laws of your country (and, in some cases, may not be as protective)."*
> — Global Privacy Statement | Intuit

Employee Offboarding Access

AI Comment: The playbook item requires that Intuit, as the vendor, maintain documented policies and systems ensuring that when one of its own employees is terminated or changes job function, that employee's access to customer data, systems, or platform is revoked or adjusted within 24 hours. Across all six documents in the review set — the Terms of Service, Global Privacy Statement, QBO Data Processing Agreement, Time/Workforce DPA, Telecom Terms, and Acceptable Use Policy — no provision specifically addresses Intuit's internal employee access lifecycle management, offboarding procedures, or any access revocation timeline upon termination or role change.

The closest provisions found are in the two DPAs (QBO DPA §4.2; Time/Workforce DPA §2.4), which confirm that Intuit's authorized personnel (including its staff, agents, and subcontractors) are required to be under confidentiality obligations. While these provisions govern behavior during the period of authorization, they are entirely silent on what happens at the point of termination or role change — they impose no duty to revoke access, let alone within 24 hours.

The general "appropriate technical and organisational measures" language in both DPAs (QBO DPA §4.1; Time/Workforce DPA §2.5) is similarly non-responsive. While such language could in theory encompass access management controls (and Intuit's security certifications, accessible via audit reports under QBO DPA §5, may cover access lifecycle management internally), these clauses provide no contractual commitment enforceable as a specific offboarding standard. They confer no right to the customer organization to demand compliance with any defined timeline.

Silence default for a High-weight item is RED. No statutory downgrade applies: California law (CCPA, Labor Code) does not specifically mandate that SaaS vendors contractually commit to 24-hour employee access revocation in their terms of service. No industry-norm downgrade is warranted either: while access management upon employee departure is standard security practice addressed in frameworks like SOC 2 Type II, the specific contractual commitment to a 24-hour window is not standard in published ToS/DPA documents.

This gap is material given QuickBooks' purpose in this deployment: bookkeeping, payroll processing, income/expense tracking, and financial reporting. Former Intuit employees retaining unauthorized access to such sensitive financial data presents meaningful risk. The reviewing legal team should consider requesting Intuit's information security policy documentation and/or negotiating a supplemental security addendum requiring contractually binding access revocation SLAs for departing or role-changing employees.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall ensure that any person that it authorizes to Process the Customer Data (including Intuit's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of …"

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Vendor's liability

AI Comment: **Overall Assessment: RED**

The vendor's liability framework partially satisfies the acceptable position on cap *amount* (the general cap in Section A is tied to 12-month fees, meeting that threshold) but **completely fails** the carve-out requirement. The acceptable position requires carve-outs from the cap for *all four* of the following: (1) data breaches, (2) breaches of confidentiality, (3) IP infringement, and (4) indemnification obligations. **None of these carve-outs appear anywhere across the ToS, DPA, or any ancillary document.** The overall rating is RED for the following compounding reasons:

1. Cap Amount — Conditionally Meets Minimum, But With Material Qualifications:
The Section A general cap (TOS §"Limitation of Liability") is set at "the greater of: (1) the fees that you paid to use the relevant Service(s) in the 12 months before the breach or (2) $100." The 12-month fee basis satisfies the minimum quantitative threshold. However, the $100 floor is a concern in early-term scenarios, and, critically, this cap is only the starting point — it is further constrained by the exclusions and Section B overrides discussed below.

2. No Data Breach Carve-Out — Directly Contrary to Acceptable Position:
No provision in any document excises data breach liability from the cap. More critically, §"Limitation of Liability" bullet 4 explicitly *excludes* from recoverable damages "damages relating to failures of telecommunications, the internet, electronic communications, corruption, security, viruses, or spyware" — language that directly encompasses the most common data breach scenarios (unauthorized access, security failure, malware). This exclusion means the vendor's data-breach liability exposure to the customer is *sub-cap*, not merely capped. QuickBooks Online DPA §10.3 provides a narrow carve-out ("In no event shall any party limit its liability with respect to any individual's data protection rights"), but this protects individual data subjects' statutory rights (e.g., right to erasure), not the *organization's* right to recover data breach damages, remediation costs, or third-party claims. This partial carve-out does not satisfy the playbook requirement.

3. No Confidentiality Breach Carve-Out:
Entirely absent across all documents. There is no language in the ToS, either DPA, or any ancillary document that excises breaches of confidentiality obligations from the cap.

4. No IP Infringement Carve-Out:
Entirely absent. The Prohibited Uses section (§"Prohibited Uses") addresses the customer's obligations not to infringe IP but creates no liability carve-out for Intuit's IP-related exposures.

5. No Indemnification Carve-Out:
The indemnification provision (§"Indemnity Obligations") runs *one-way* — the customer indemnifies Intuit, not vice versa. There is no mutual indemnification, and no carve-out from the cap for any indemnification-related liability.

6. Section B Overrides Further Restrict Liability for Key Use-Case Services Below the General Cap:
Section B Terms explicitly prevail over Section A. For the three primary service categories relevant to the stated use case (payroll processing, bookkeeping, and contractor payments), the Section B terms impose liability limits more restrictive than the general 12-month fee cap — in each case limiting Intuit's sole obligation to *correcting the error only*, with no monetary recovery. This is a significant aggravating factor given the intake description (bookkeeping, income/expense tracking, payroll, financial reports).

7. Exclusive Remedy Clause:
§"Limitation of Liability" states "This Agreement sets forth your exclusive remedy with respect to the Platform and its use," reinforcing the caps and exclusions as an absolute ceiling.

Ideal Preference: The preference for uncapped vendor liability or a super-cap for data-breach liability is not remotely

met. Intuit's posture moves in the *opposite* direction — sub-cap exclusions for data breach scenarios and near-zero liability for payroll/bookkeeping errors.

Confidence: HIGH. The liability provisions are explicit, comprehensive, and unambiguous. No plausible reading of any document supports the existence of the required carve-outs.

— Superseding reasoning —
Multiple superseding determinations apply. First, Section B Terms expressly prevail over Section A Terms per the opening paragraph of Section B (PIF 2). This means the service-specific liability restrictions in Section B (payroll, bookkeeping, contractor payments — PIFs 3, 4, 5) each supersede the general Section A cap (PIF 0) for their respective service areas under the SPECIFIC_OVER_GENERAL and EXPLICIT_OVER_IMPLICIT principles. Second, the QuickBooks Online DPA (Document 3) §11.3 establishes that the DPA prevails over the Agreement for data processing claims; accordingly, DPA §10 (PIF 6) governs the liability framework for Business Connection Data processing claims, but §10.1 incorporates the Agreement's caps by reference rather than displacing them. The DPA's §10.3 adds a narrow individual-rights carve-out atop the Agreement's caps. The net governing language for each service area is set out in the supersedingDetails array below.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The total aggregate liability of Intuit and our third party providers, licensors, distributors or suppliers ("Intuit Parties") arising out of or relating to this Agreement is limited to the greater of…"
2. "The Intuit Parties won't be responsible for the following:

- Loss of data, profits, revenues, business opportunities, goodwill or anticipated savings;
- Indirect, incidental, or consequential loss;
-…"
3. "Your use of the Services provided by Intuit (as defined in the Section A Terms) and described below are subject to the Section A Terms above and these Additional Terms and Conditions ("Section B Terms…"
4. "10.1Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of I…"

> *"Notwithstanding anything to the contrary in the Section A Terms, if any Intuit error occurs in processing Payroll Payments, our only responsibility will be to make the correct payment or file the correct report and pay any resulting tax interest or penalty."*
> — QBO Terms of Service for QuickBooks - US
> *"Notwithstanding anything to the contrary in the Section A Terms, if any Intuit error occurs in performing the QuickBooks Live Expert Services, our only responsibility will be to correct the error in QuickBooks Online for the month the error occurred."*
> — QBO Terms of Service for QuickBooks - US
> *"Notwithstanding anything to the contrary in Section A, if Intuit makes any errors in performing Contractor Payments Services, our only responsibility will be to make the correct payment to the independent contractor or file the correct Form 1099."*
> — QBO Terms of Service for QuickBooks - US

Security Training

AI Comment: The playbook requires a specific contractual commitment that vendor employees who access customer data must attend security training at least annually. A thorough review of all five provided documents — the QBO Terms of Service, Global Privacy Statement, QBO Data Processing Agreement, QuickBooks Time & Workforce DPA, and the Acceptable Use Policy — reveals no language that explicitly addresses employee security training, its scope, or its frequency.

The closest relevant language appears in the QBO DPA (Section 4.1), which obligates Intuit to implement "appropriate technical and organisational measures" including a process for "regularly testing, assessing and evaluating the effectiveness of technical and organisational measures." Section 4.2 further requires that authorized persons processing Business Connection Data "shall be under an appropriate obligation of confidentiality." The Time/Workforce DPA (Section 2.5) contains substantively identical language. These provisions evidence a general security framework but do not constitute a commitment to employee security training — they address process controls, not human training obligations. "Confidentiality obligation" is a duty of non-disclosure, not a training requirement.

The QBO DPA also references Intuit's Security Center (security.intuit.com) for further detail on technical and organizational measures. While external security certifications (e.g., SOC 2 Type II) that Intuit may hold would typically require security awareness training, those certifications are not contractually incorporated into the reviewed documents, and reliance on external documentation not incorporated by reference does not satisfy the playbook requirement.

Because the contract is silent on the specific requirement and the item weight is Medium, the default classification is YELLOW per the silence-handling framework. No California or federal statute was identified that independently mandates annual vendor-employee security training equivalent to the playbook's acceptable position. While security awareness training is a recognized industry practice, the absence of any contractual commitment — even a general one — means the acceptable position is not met. The practical risk is moderate: Intuit is a large financial-technology company with extensive security infrastructure, making it probable (though not contractually guaranteed) that employee training occurs.

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and*

severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymisation or encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."
— DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."
— QuickBooks Time & Workforce (Time/Payroll) DPA

Indemnification – Vendor to Our Company

AI Comment: The acceptable position requires the vendor (Intuit) to indemnify the customer for intellectual property infringement claims and data breaches. The document set affirmatively contradicts both components of this requirement — this is not mere silence.

IP Indemnification: No vendor-to-customer IP indemnification exists anywhere across all five documents. More critically, the ToS Disclaimers section explicitly disclaims any warranty of non-infringement: "we do not provide implied warranties, such as the implied warranties of merchantability, fitness for a particular purpose, or non-infringement." This is a direct contractual contradiction — Intuit will not even warrant that the platform does not infringe third-party IP, let alone indemnify the customer for resulting claims. For a financial platform like QuickBooks that relies on proprietary software components, this exposes the customer to uncovered IP litigation risk.

Data Breach Indemnification: The ToS Limitation of Liability section explicitly lists "Loss of data, profits, revenues, business opportunities, goodwill or anticipated savings" and "Indirect, incidental, or consequential loss" among the categories for which Intuit accepts no responsibility. This affirmatively bars any financial recovery for data breach impacts. The QBO DPA (Document 3) does address security incidents, but only through notification and response assistance obligations — not indemnification. Moreover, DPA Section 10.1 explicitly ties all DPA liability back to "the exclusions and limitations of liability set forth in the Agreement," incorporating the same ToS caps that exclude data loss. The Time/Workforce DPA (Document 4) is structurally identical on this point.

Indemnification Direction is Entirely Reversed: The Agreement's only indemnification obligation runs customer !' vendor ("You will indemnify and hold harmless the Intuit Parties..."), not vendor !' customer. No reciprocal obligation exists anywhere in the document set.

Combined Assessment: The contract actively contradicts the acceptable position on both IP and data breach components through: (1) explicit disclaimer of non-infringement warranty; (2) explicit exclusion of data loss from Intuit's liability; (3) unidirectional indemnification structure (customer indemnifies vendor only); and (4) DPA liability framework deferring to Agreement's caps. Classification: RED. For a Medium-weight item, this represents moderate risk requiring documented justification. Given that QuickBooks is being used to process financial data and payroll, the complete absence of data breach indemnification is a practically significant gap.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "If Intuit becomes aware of an actual Security Incident that involves Business Connection Data, Intuit will: (a) notify Customer of the Security Incident without undue delay; (b) take appropriate steps…"
2. "Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liabi…"

"You will indemnify and hold harmless the Intuit Parties for any losses, damages, judgments, fines, costs and expenses (including legal fees) in connection with any claims arising out of or relating to your unlawful or unauthorized use of the Platform or violation of this Agreement. Intuit reserves the right, in its sole discretion and at its own expense, to assume the exclusive defense and control of any claims. You agree to reasonably cooperate as requested by Intuit in the defense of any claims."
— QBO Terms of Service for QuickBooks - US
"Unless required by law, we do not provide implied warranties, such as the implied warranties of merchantability, fitness for a particular purpose, or non-infringement."
— QBO Terms of Service for QuickBooks - US
"Limitation of Liability," "Indemnity Obligations," "Disputes," and "General Terms (Miscellaneous)"."
— QBO Terms of Service for QuickBooks - US

Vendor Audit Rights

AI Comment: The playbook requires that the customer hold "the right to audit Vendor's systems and compliance with DPA." Both the QBO DPA (Document 3, §5) and the Workforce/Time DPA (Document 4, §2.11) expressly address audit and oversight rights, but neither grants a genuine audit right as that term is ordinarily understood in commercial contracting.

Intuit instead substitutes a two-part inspection-lite mechanism: (1) allowing the customer to review Intuit's own existing security audit reports, and (2) permitting the customer to submit written questions to which Intuit will respond. For Workforce/Time services specifically, the Workforce DPA further constrains this mechanism to written questions only — with no mention of report review — and caps the exercise of that right to once per calendar year (§2.11).

What is absent is material: (a) a right to conduct on-site or remote direct-access audits of Intuit's systems; (b) a right to engage the customer's own or a designated third-party auditor; (c) any obligation on Intuit to provide system-level access, artifacts, or evidence beyond what Intuit itself curates in its published reports; and (d) any right to inspect actual controls or processes in operation. "Reviewing audit reports" is categorically different from "auditing" — the customer is reviewing Intuit's own curated output rather than exercising independent verification.

This constitutes partial coverage of the playbook item — the audit/oversight subject is expressly addressed, and some compliance verification pathway exists — but the protection is materially narrower than the acceptable position. Classification is YELLOW (not RED) because the topic is not ignored; a verification mechanism exists. However, the mechanism does not meet the acceptable position as written. For a High-weight item, this warrants documented legal assessment before acceptance.

Scope note: The two DPAs govern different services and do not conflict with each other. Document 3 governs core QuickBooks Online services; Document 4 governs Workforce, Time, and Contractor Payments services. Both are independently applicable given the intake brief's use cases (bookkeeping, payroll, financial reports). Neither supersedes the other.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"
2. "Intuit shall respond to any written audit questions related to Intuit's security practices submitted to it by Customer, provided that Customer shall not exercise this right more than once per year."

Non-Solicitation of Employees

AI Comment: The QuickBooks Terms of Service (all of Section A and the extensive Section B product-specific terms), the QuickBooks Online DPA, the QuickBooks Time & Workforce DPA, the Global Privacy Statement, the Intuit Telecom Specific Terms, and the Acceptable Use Policy are collectively and entirely silent on any mutual non-solicitation of employees provision. No clause in any document restricts either party from recruiting, soliciting, or hiring the other party's personnel through any channel whatsoever.

This silence is affirmatively favorable and diverges from the typical "silence = gap" posture that the Medium-weight default (YELLOW) assumes. Here, silence means no restriction is contractually imposed on the reviewing organization. The acceptable position requires that if a non-solicitation clause exists, it must carve out instances where applicants respond to general public postings — a protection that ensures the reviewing organization can respond to organic, publicly-initiated applications without violating the agreement. Since there is no non-solicitation clause at all, that carve-out is not needed; the reviewing organization already has complete freedom to hire Intuit employees who respond to any general posting. This outcome exceeds the acceptable position and also fully meets the ideal preference of "no limitations on solicitation," including for recruiter-referred candidates.

Under the governing jurisdiction of California, this favorable posture is further buttressed by California Business and Professions Code § 16600, as substantially strengthened by SB 699 (effective January 1, 2024) and AB 1076. These statutes void employee non-solicitation provisions between businesses in California, meaning that even if such a clause existed in the contract, it would face significant enforceability challenges in this jurisdiction. The complete contractual silence eliminates any ambiguity entirely.

One section of the ToS was specifically reviewed for potential confusion: Part F, Section 8.a (Job Postings / Recruiting and Onboarding Services). This section imposes rules on the customer when posting job listings through the QuickBooks Workforce platform but is entirely directed at the customer's own recruitment activities using the QB platform — it is not a mutual non-solicitation clause between Intuit and the customer. It creates no restriction on either party's ability to solicit the other's employees.

Because the complete absence of any restriction achieves the practical legal effect that is superior to both the acceptable position and the ideal preference, this item is classified GREEN with aiPreferenceMet = true. The silence default downgrade mechanism is inapplicable; this is a case where silence is unambiguously beneficial and produces a better outcome than any affirmative language would have provided. The silenceDowngrade field is null for that reason.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.

1. "This DPA reflects the parties' agreement with respect to Intuit's processing and security of Personal Information as a Processor, as further set forth in the Agreement."

> *"This Agreement, including any Section B terms, is the entire agreement between you and Intuit and replaces all prior understandings, communications and agreements, oral or written, regarding its subject matter."*
> — QBO Terms of Service for QuickBooks - US
> *"In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Anti-Virus Solution

AI Comment: The acceptable position for this High-weight item requires a vendor commitment that all authorized computer systems maintain an anti-virus solution. After exhaustive review of all five substantive documents (Terms of Service, Global Privacy Statement, QBO Data Processing Agreement, QuickBooks Workforce/Time DPA, and Acceptable Use Policy), no provision specifically addresses anti-virus or endpoint protection controls on Intuit's computer systems.

The silence default for a High-weight item is RED.

Silence downgrade evaluation:

Statute basis: No California statute (CCPA, Cal. Civ. Code § 1798.82, or comparable) specifically mandates anti-virus software on vendor computer systems. California's reasonable-security standard is too general to provide equivalent contractual protection against the absence of a specific enumerated control. No downgrade on statute basis.

Industry norm basis: While it is standard SaaS market practice to commit to general "appropriate technical and organizational measures" (TOMs) rather than enumerating specific security controls like anti-virus in public-facing T&Cs and DPAs, that norm does not establish low practical risk sufficient to justify a downgrade here. Critically, the ToS Section A Disclaimers affirmatively disclaim any warranty that the Platform is "free from any viruses or other harmful components" (1-144). This explicit disclaimer, combined with the absence of any anti-virus-specific commitment anywhere in the document set, means the customer has no contractual assurance—express or implied—that Intuit's authorized systems run anti-virus solutions. Practical risk is not low when the vendor has specifically disclaimed virus-related warranties. No downgrade on industry norm basis.

The two DPA provisions (Doc 3, § 4.1; Doc 4, § 2.5) commit Intuit to "appropriate technical and organisational measures" and reference the Intuit Security Center for details, but these general commitments do not functionally satisfy a specific anti-virus requirement because: (a) "appropriate TOMs" is a standard of reasonableness that could be satisfied without anti-virus in certain architectures; (b) the security audit reports referenced are not part of this contract and are not legally binding commitments; and (c) the ToS disclaimer actively undercuts any inference that anti-virus is provided. These provisions address the same general topic (security) but with materially weaker and non-specific protection relative to the playbook item's acceptable position.

Overall classification: RED. The contract is silent on the specific control required, the weight is High, and no statutory or industry-norm downgrade is warranted. The reviewing legal professional should seek contractual confirmation (e.g., via an Order Form supplement, security addendum, or SOC 2 Type II report with anti-virus control coverage) before accepting this vendor for use with sensitive financial data.

> *"We do not warrant that the Platform is error-free, secure, or free from any viruses or other harmful components."*
> — QBO Terms of Service for QuickBooks - US
> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA
> *"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."*
> — Global Privacy Statement | Intuit

Data Retention & Deletion

AI Comment: The acceptable position requires two specific, measurable commitments: (1) deletion of requested data from production systems within 30 days of request, and (2) deleted data cycling out of backups within 364 days. The document set — spanning the ToS, Privacy Statement, QBO DPA, and Time/Workforce DPA — collectively addresses data deletion but fails to commit to either specific timeframe. This warrants a YELLOW classification: the topic is meaningfully addressed across multiple instruments, but the protection is materially weaker than the acceptable position.

In-service deletion requests: The ToS directs users to account settings or the Global Privacy Statement for deletion (no timeframe). The Privacy Statement establishes that data is retained "as long as it is necessary" by default and, even after a deletion request is submitted, Intuit may continue to retain personal information for legal compliance, legal claims, and fraud protection — broad carve-outs that could indefinitely defer deletion. No 30-day production deletion commitment exists. For California users (the governing jurisdiction), the CCPA provides a statutory right to deletion, but the CCPA's response window of 45 days (extendable to 90 days) is itself longer than the 30-day acceptable threshold and applies only to "personal information," not necessarily all Business Connection Data.

Post-termination deletion: The QBO DPA (Section 7) obligates Intuit to provide "reasonable measures" for deletion of Business Connection Data upon termination and commits to "eventually" delete backup copies "in accordance with Intuit's deletion policies" — but those policies are neither defined in the agreement nor referenced to any public document. The Time/Workforce DPA (Section 2.10) similarly defers to "Intuit's data retention and destruction procedures and timeframes" without defining them. Neither instrument specifies any deletion timeframe.

Aggregated/derived data carve-out: The ToS explicitly reserves Intuit's right to collect, own, and use deidentified and aggregated data derived from customer content "without restriction." This data is excluded from any deletion obligation, which further narrows the effective scope of deletion rights.

Superseding logic: The QBO DPA (Doc 3, §11.3) establishes that in any conflict between the DPA and the Agreement, the DPA prevails for Business Connection Data. The Time/Workforce DPA (Doc 4) contains a parallel control clause for Time/Workforce/Contractor Payments data. Accordingly, the DPA provisions on deletion govern over the general ToS deletion reference for those data categories.

Summary of gap: Neither the 30-day production deletion threshold (acceptable) nor the 10-day threshold (ideal preference) is contractually committed anywhere in the document set. Backup deletion timelines are delegated to Intuit's internal, unspecified policies. This is a material gap for a HIGH weight item, particularly given QuickBooks' use for processing payroll, financial transactions, and sensitive business records.

— Superseding reasoning —
Two superseding determinations apply. First, Section 11.3 of the QBO DPA (Doc 3) expressly establishes document hierarchy: "(i) SCCs; then (ii) this DPA; and then (iii) the Agreement." For deletion obligations covering Business Connection Data processed under the QBO agreement, the QBO DPA Section 7 governs over the ToS's general account-settings deletion instruction. Second, the introductory clause of the Time/Workforce DPA (Doc 4) states: "In the event of any discrepancies between the terms of this DPA and the Agreement with respect to the Processing of Customer Data, this DPA shall control." For Customer Data in Time, Workforce, and Contractor Payments services, Section 2.10 of that DPA governs over the ToS deletion reference. Both superseding instruments still fail to supply the required timeframes — the superseding does not improve the overall classification. The Privacy Statement (Doc 2) is not superseded: it operates as the governing instrument for general personal data (non-Business Connection Data) and for in-service deletion requests by end users.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "You may have the right, under certain circumstances, to request that we delete the Personal Information you have provided to us. You may delete your Personal Information in the Privacy section of your…"
2. "At Customer's election, Intuit shall return or destroy all Customer Data in its possession or control (including in the possession of any Subprocessor) in accordance with Intuit's data retention and d…"

> *"Termination**"*
> — QBO Terms of Service for QuickBooks - US
> *"Content and Data"*
> — QBO Terms of Service for QuickBooks - US
> *"Data retention**"*
> — Global Privacy Statement | Intuit
> *"There may be occasions where we are unable to fully delete, anonymize, or de-identify your personal information due to technical, legal, regulatory compliance, or other operational reasons. Where this is the case, we will take reasonable measures to securely isolate your personal information from any further processing until such time as we are able to delete, anonymize, or de-identify it."*
> — Global Privacy Statement | Intuit
> *"Section 7 (Return or Deletion of Data) of this DPA."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Automatic Renewal

AI Comment: The contract meets both prongs of the acceptable position — (1) at least 30 days' advance notice before renewal, and (2) an unconditional right to cancel before renewal — and is therefore classified GREEN.

Notice prong: Section A's "Payment & Cancellations" clause explicitly provides that for annual subscriptions Intuit will send a renewal reminder "no less than thirty (30) days and no more than sixty (60) days before your subscription term ends, or otherwise as required by applicable law." This satisfies the 30-day minimum stated in the acceptable position and, at the upper bound (60 days), exceeds it. The "or otherwise as required by applicable law" catch-all further preserves compliance with any jurisdiction-specific mandate (e.g., California ARL § 17602(a)(3) requires at least 15 days' notice for annual renewals — Intuit's floor of 30 days comfortably exceeds that).

Cancellation right prong: Section A unambiguously states that "you can cancel a subscription at any time," with cancellations taking effect at the end of the current subscription period (not mid-period). This satisfies the right-to-cancel-before-renewal requirement. Section B product-specific terms (QuickBooks Live Expert Services, Intuit Accountant Suite) reinforce this by providing explicit in-product cancellation pathways and confirming the same "end of subscription period" effective date.

Noted gap — non-annual intervals: The 30-day advance renewal reminder is expressly scoped to annual subscriptions. For monthly or other shorter recurring-interval subscriptions, no advance per-cycle renewal notice is stated. This gap does not change the classification because: (a) the item weight is "Acceptable to Deviate" (lowest threshold); (b) California Automatic Renewal Law does not require advance notice for monthly renewals, only clear disclosure at enrollment; (c) industry norm for monthly SaaS subscriptions does not include per-renewal advance notice; and (d) the unconditional cancellation right applies to all subscription types regardless of billing interval. The practical consumer-protection concern — surprise annual renewal — is the scenario the 30-day notice requirement is designed to address, and Intuit's terms squarely cover it.

Document hierarchy: Section B Terms prevail over Section A Terms in the event of direct conflict (Section B preamble). The Section B product-specific cancellation provisions are supplementary and harmonious with Section A's renewal notice framework — they provide cancellation mechanics without displacing or conflicting with the 30-day notice obligation. No superseding determination is required.

> *"You may be charged a subscription fee in advance on an annual basis or other recurring interval disclosed to you prior to your purchase. For annual subscriptions, we will send you a reminder with the then-current subscription fee no less than thirty (30) days and no more than sixty (60) days before your subscription term ends, or otherwise as required by applicable law."*
> — QBO Terms of Service for QuickBooks - US
>
> *"Your payment to Intuit will automatically renew at the end of the applicable subscription period but you can cancel a subscription at any time. Subscription cancellations will take effect the day after the last day of the current subscription period. If you cancel in the middle of a subscription period, you will be able to continue to access and use the applicable Service until the end of your subscription period."*
> — QBO Terms of Service for QuickBooks - US
>
> *"Following any free trial period, your account will be automatically charged the applicable subscription fee at the recurring subscription period you selected until you cancel. You may cancel Live Priority at any time before your next billing date. To cancel, go to 'Account Settings' and 'Billing & Subscription' and cancel your subscription. Your cancellation will become effective at the end of your subscription period. You will not receive a prorated refund."*
> — QBO Terms of Service for QuickBooks - US
>
> *"Subscription cancellations will take effect the day after the last day of the current subscription period. If you cancel in the middle of a subscription period you will be able to continue to access and use the applicable Service until the end of your subscription period. We do not provide refunds or credits for any cancellations or partial subscription period."*
> — QBO Terms of Service for QuickBooks - US

Ownership of Custom Deliverables

AI Comment: The acceptable position requires that the vendor assign ownership of any custom deliverables to the customer, while permitting the vendor to retain its own pre-existing and background IP. The QuickBooks terms affirmatively conflict with this position across all documents reviewed.

No IP assignment clause exists anywhere in the document set. Instead, the terms operate in the opposite direction: Intuit explicitly retains all right, title, and interest in the Platform and everything it builds; customers receive only a personal, limited, nonexclusive, nontransferable, revocable license; and Intuit asserts outright ownership of deidentified and aggregated data it derives from customer usage and content.

Three categories of potential "custom deliverables" arise in the QuickBooks context, and the terms fail the acceptable position in each:

1. **Core SaaS Platform / Software**: Customers receive only a revocable, non-exclusive license. The software is "licensed, not sold." No assignment of any kind is made to the customer. Intuit retains all residual rights.

2. **AI-Generated and Customizable Work Product (Workforce Services)**: Intuit explicitly states that AI-generated outputs such as job descriptions, HR policies, and contract templates were not "prepared specifically for you or on your behalf" — affirmatively disclaiming any custom nature. No IP assignment is provided for these outputs.

3. **QuickBooks Live Bookkeeping Work Product**: Bookkeepers perform categorization, reconciliation, and produce

financial statements within the customer's QuickBooks account. While the outputs reside in the customer's account (implying de facto control as the customer's "Content"), there is no explicit IP assignment of Intuit's authorship interests in the work product. The sole remedy for errors is correction in QuickBooks Online for the affected month — not an IP transfer.

Additionally, Intuit's ownership of deidentified/aggregated data derived from customer content and usage — with no restrictions on use — further underscores the one-sided IP framework.

Notably, Intuit's general Content and Data terms do preserve the customer's pre-existing IP in content the customer brings to the platform ("Your Content remains yours"). This is consistent with the playbook's allowance for the vendor to retain its own background IP. However, no reciprocal obligation runs the other way: Intuit does not assign what it creates.

The Section B Product Specific Terms formally prevail over Section A in cases of conflict (explicit hierarchy clause), but neither Section A nor any Section B term contains IP assignment language favoring the customer. Document hierarchy does not cure the substantive gap.

This is a HIGH weight item. The absence of any IP assignment clause for custom deliverables, combined with Intuit's affirmative retention of all Platform IP and ownership of derived data, directly conflicts with the acceptable position. Senior legal justification is required to accept this risk. The practical severity is modulated by QuickBooks' primary nature as a standard SaaS product (most customers do not commission bespoke software from Intuit), but organizations using QuickBooks Live Bookkeeping or Workforce AI-generation features may have a genuine exposure if disputes arise over authorship of work product.

— Superseding reasoning —
The Section B Product Specific Terms contain an explicit hierarchy clause stating they prevail over Section A in cases of direct conflict or inconsistency. This clause is applied below as a superseding determination with respect to general Platform IP provisions. However, the superseding analysis does not alter the item-level classification because neither Section A nor Section B contains any language assigning custom deliverables to the customer — the outcome is RED under both documents.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Conditioned upon your compliance with the terms and conditions of this Agreement (including all payment obligations), Intuit grants you a personal, limited, nonexclusive, nontransferable, revocable li…"
2. "Intuit may collect, derive or generate deidentified and/or aggregated data regarding your usage of or the performance of the Platform, including data derived from your Content. Intuit will own all suc…"

> *"As between you and Intuit, Intuit and its licensors retain all right, title or interest in and to the Platform, except for the rights granted to you."*
> — QBO Terms of Service for QuickBooks - US
> *"The Workforce Services include services or features that generate customized results based on your inputs or selections, such as configurable account settings, content created with artificial intelligence (e.g. job descriptions, summaries, and responses provided by Digital Assistants, as defined in Section A), customizable HR workflows, and a variety of sample documents (e.g. policies, forms and contract templates). While Intuit has developed such features with a variety of situations in mind, none have been prepared specifically for you or on your behalf, they may not meet your exact needs (business, legal or otherwise), and your use of such features with your own configurations and content may result in new and untested results and outcomes. You are responsible for assessing and verifying the suitability of any such features and results prior to using them for your business."*
> — QBO Terms of Service for QuickBooks - US
> *"Notwithstanding anything to the contrary in the Section A Terms, if any Intuit error occurs in performing the QuickBooks Live Expert Services, our only responsibility will be to correct the error in QuickBooks Online for the month the error occurred."*
> — QBO Terms of Service for QuickBooks - US
> *"These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms."*
> — QBO Terms of Service for QuickBooks - US

Termination for Cause

AI Comment: The acceptable position requires that the customer (reviewing organization) have the right to terminate the Agreement if Intuit (the vendor) breaches. The documents collectively address termination, but not in a way that squarely meets the playbook item's standard.

What the contract provides:
The Terms of Service grant the customer an at-will cancellation right ("you can cancel a subscription at any time"), but this is not framed as—or tied to—a breach-triggered termination mechanism. Critically, at-will cancellation under these terms (1) only takes effect at the end of the current subscription period, and (2) entitles the customer to no refund of pre-paid fees regardless of whether the cancellation is motivated by vendor breach. This is a weaker protection than a proper termination-for-cause clause, which typically provides for immediate or near-immediate effect and may preserve pre-paid fee recovery rights.

The termination provisions are structurally asymmetric: Intuit can "terminate this Agreement (and your account) or suspend the Platform at any time in our discretion," while the customer's exit right is limited to at-will subscription cancellation under the standard subscription-period-end mechanics.

Narrow DPA-based breach-triggered termination rights:
The QuickBooks Online DPA (Document 3, §6.4) provides a limited breach-triggered termination right, but only in the narrow context of Intuit's non-compliance with the Standard Contractual Clauses for EU/UK data transfers. Similarly, the Workforce/Time DPA (Document 4, §2.6) permits termination if the customer refuses a new sub-processor appointment. Neither constitutes a general termination-for-cause right upon Intuit's breach of the main commercial agreement.

Statutory background:
Under California law (the governing law per ToS §"Governing Law"), a party's material breach of contract generally entitles the non-breaching party to terminate. This provides some background protection. However, reliance on an implied statutory right rather than a contractual provision creates risk: the customer would bear the burden of demonstrating material breach in any dispute, without benefit of a defined cure period or explicit contractual right.

Overall assessment:
The contract addresses termination but provides no explicit breach-triggered termination right for the customer against Intuit. The at-will cancellation right is a functionally broader but structurally weaker substitute: broader because it requires no cause, weaker because it lacks immediate effect and offers no fee recovery. Given the "Acceptable to Deviate" weight, this gap is moderate in severity. Classification: YELLOW.

— Superseding reasoning —
The DPA (Document 3) contains an express precedence clause (§11.3) stating that in any conflict between the DPA and the Agreement, the DPA controls, and the SCCs control over both. Accordingly, the narrow breach-triggered termination rights in DPA §6.4 (SCC non-compliance context) supersede any inconsistent general ToS termination provisions for that specific scope. Outside that SCC-specific scope, the general ToS termination provisions govern. No broader conflict among the general ToS termination provisions requires resolution.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Upon expiration of your subscription or cancellation of your account, or Intuit's termination of your account or this Agreement, you must immediately stop using the Platform and pay all fees for Platf…"
2. "If Customer refuses to consent to Intuit's appointment of a third-party Subprocessor relating to the protection of the Customer Data, Customer may elect to suspend or terminate the Agreement, includin…"

> *"This Agreement is effective until your subscription expires or you cancel your account or Intuit terminates this Agreement (or your account). Intuit may terminate this Agreement (and your account) or suspend the Platform at any time in our discretion."*
> — QBO Terms of Service for QuickBooks - US
> *"Your payment to Intuit will automatically renew at the end of the applicable subscription period but you can cancel a subscription at any time. Subscription cancellations will take effect the day after the last day of the current subscription period. If you cancel in the middle of a subscription period, you will be able to continue to access and use the applicable Service until the end of your subscription period. We do not provide refunds or credits for any cancellations or partial subscription period."*
> — QBO Terms of Service for QuickBooks - US
> *"If Customer intends to suspend the transfer of European Data and/or terminate the affected parts of the Service, it shall first provide notice to Intuit and provide Intuit with a reasonable period of time to cure such non-compliance, during which time Intuit and Customer shall reasonably cooperate to agree what additional safeguards or measures, if any, may be reasonably required. Customer shall only be entitled to suspend the transfer of data and/or terminate the affected parts of the Service for non-compliance with the SCCs if Intuit has not or cannot cure the non-compliance within a reasonable period."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Password Encryption

AI Comment: The playbook item requires that passwords are always stored in encrypted form — a categorical, unconditional commitment covering all password types in vendor custody.

Across the document set, three distinct clusters of relevant language exist: (1) an explicit encryption commitment for third-party login credentials stored under the Data Receipt Service (Doc 1, §D); (2) a broader general security commitment using "appropriate technical and organizational measures" for third-party credentials in the Data Transfer Service (Doc 1, §B); and (3) DPA-level security provisions that include encryption as one among several listed technical safeguards for personal data, while simultaneously classifying "account passwords" as Sensitive Data that customers should not provide (Doc 3, §4.1 / §1 Sensitive Data definition).

None of these provisions constitutes a clear, categorical commitment that Intuit's own user account passwords (i.e., QuickBooks platform login credentials) are always stored in encrypted form. The strongest language — "login credentials will be encrypted" — is scoped exclusively to third-party service credentials used for data import, not to QuickBooks account authentication credentials. The DPA security provisions list encryption as an appropriate measure "as appropriate" among several options (pseudonymization or encryption), which is architecturally permissive language rather than an absolute guarantee. The Global Privacy Statement offers only general safeguard language with an explicit disclaimer that security cannot be completely ensured.

The High weight of this item means the partial and scoped coverage of password encryption — rather than a universal, explicit guarantee — warrants a YELLOW classification. The applicable position calls for "always" and encompasses all passwords; the contract delivers that assurance only for a narrowly defined category of third-party credentials and relies on

general, non-categorical DPA security language for everything else.

Superseding note: The DPA (Doc 3) governs over the ToS (Doc 1) on data-processing security matters per §11.3 of the DPA; within the ToS, Section B Terms prevail over Section A Terms per the ToS opening clause. The DPA security section therefore controls how security obligations are read, and it is the DPA's conditional/non-absolute encryption language that governs the strength of the commitment.

— Superseding reasoning —
Within the ToS (Doc 1), Section B Terms expressly prevail over Section A Terms in the event of conflict. The DPA (Doc 3, §11.3) establishes a further hierarchy in which (i) SCCs, then (ii) the DPA, then (iii) the Agreement govern on data-processing matters. Accordingly, the DPA's security provisions (§4.1) — which include encryption as one of several listed measures for personal data — supersede the more general "appropriate technical and organizational measures" language in the ToS Data Transfer Service clause (Doc 1, §B). The Data Receipt Service's explicit "will be encrypted" language (Doc 1, §D) applies to a narrower, specific category of third-party import credentials and is not overridden by the DPA, as it represents a specific, contextual commitment rather than a conflicting general provision; under the specific-over-general principle, this language governs for that specific data category.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. ""Sensitive Data" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit, genetic, biometric or health i…"

> *"We will use appropriate technical and organizational measures to secure this data consistent with applicable data privacy and protection laws or regulations. In addition, we will only use these credentials in order to share data with the Third-Party Service you have indicated."*
> — QBO Terms of Service for QuickBooks - US
> *"Maintained login credentials will be encrypted and used in connection with importing your data to our Service otherwise with your permission."*
> — QBO Terms of Service for QuickBooks - US
> *"You are responsible for securely managing your Account Information, including your user ID and any password(s) for the Platform."*
> — QBO Terms of Service for QuickBooks - US
> *"Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"Other than as expressly contemplated by the Services or requested by Intuit, Customer will not provide (or cause to be provided) any Sensitive Data to Intuit for processing under the Agreement, and Intuit will have no liability whatsoever for such unauthorized Sensitive Data, whether in connection with a Security Incident or otherwise."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
> *"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information. However, despite these controls, we cannot completely ensure or warrant the security of your personal information."*
> — Global Privacy Statement | Intuit
> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA

Exclusivity

AI Comment: A thorough review of all five documents in the set — the QuickBooks Terms of Service (Section A and Section B Product Specific Terms), the Global Privacy Statement, the QBO Data Processing Agreement, the QuickBooks Workforce and Time DPA, the Intuit Telecom Specific Terms, and the Acceptable Use Policy — found no exclusivity provision of any kind. Intuit does not restrict the customer from simultaneously using competing accounting software, payroll providers, bookkeeping services, or payment processors. No clause imposes a requirement that QuickBooks or any Intuit product be the customer's sole or primary solution in any category.

The contract structure is affirmatively consistent with non-exclusive use. The Data Transfer Service provision (Part B, Section B of the ToS) expressly permits the customer to connect the QuickBooks account to non-Intuit third-party services. The Third Party Services and Products provision (Section A) further confirms that the platform is designed to interoperate with external solutions. These provisions collectively establish that Intuit contemplates — and accommodates — customers who use QuickBooks alongside other products, directly contradicting any notion of exclusivity.

Restrictions found in the agreement (use limited to "internal, lawful and non-commercial purposes"; geographic restrictions on Workforce and Contractor Payments; Merchant Application scope limits on QuickBooks Payments) are operational constraints on how Intuit's services are used, not exclusivity requirements that would preclude the customer from engaging competing vendors.

The document hierarchy clauses (Section B Terms prevail over Section A Terms; SCCs !' DPA !' Agreement) are noted but do not affect this finding, as none of those tiers introduce exclusivity obligations at any level.

The playbook requires that exclusivities not be accepted. The absence of any exclusivity provision across the entire contract set satisfies this requirement. Classification: GREEN.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "We may provide you with the opportunity to connect your account or our Service with non-Intuit-owned services ("Third Party Services") (such functionality, the "Data Transfer Service"). To do so, you …"
2. "Intuit shall process Business Connection Data, as further described in Annex A (Details of Data Processing) of this DPA, only in accordance with Customer's documented lawful instructions as set forth …"

> *"The Platform may also include information about or offers for third-party services or products or allow you to connect your account to or otherise access third-party services or products. Intuit does not warrant, and is not responsible for, such third party services and products or claims made about them, or the actions or inactions of any third party."*
> — QBO Terms of Service for QuickBooks - US
>
> *"You agree that your data sharing will comply with all terms and conditions of the other services and you will not share data in any manner that is unlawful or would infringe or violate the rights of Intuit or any other party."*
> — QBO Terms of Service for QuickBooks - US

Security Certifications

AI Comment: The document set partially addresses the security certification playbook item but falls materially short of the acceptable position. The playbook requires the vendor to contractually commit to maintaining a current SOC 2 Type II report or ISO 27001 certification covering the services, available on customer request.

The closest provisions appear in two DPAs. The QBO DPA (Section 5) commits to making "security audit reports" available for review via the Intuit compliance page (intuit.com/compliance) and to responding to written questions about data processing and protection. The Time/Workforce DPA (Section 2.11) provides a separate right to submit written audit questions, capped at once per year. These provisions partially address the "available on request" element of the requirement.

However, neither document specifically names SOC 2 Type II or ISO 27001 as the form of certification Intuit will maintain. The generic phrase "security audit reports" does not create an enforceable contractual obligation to produce or maintain a SOC 2 Type II report or ISO 27001 certificate specifically. While Intuit publishes SOC 2 reports on its compliance page in practice, the contract does not guarantee that a SOC 2 Type II report (as opposed to any other type of audit artefact) will be produced on request. Additionally, the Time/Workforce DPA's once-per-year cap on audit inquiries is a further restriction not contemplated by the playbook's standard.

Because the topic is addressed — audit reports are referenced and a review mechanism exists — this is not a silence finding. However, the protection offered is narrower and vaguer than the acceptable position, warranting a YELLOW classification. For a High-weight item, this requires documented assessment and review. The reviewing attorney should consider seeking a written assurance or side letter from Intuit confirming that current SOC 2 Type II reports are available for customer review, which would resolve the gap without requiring a contractual amendment.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"
2. "Intuit shall respond to any written audit questions related to Intuit's security practices submitted to it by Customer, provided that Customer shall not exercise this right more than once per year."

Warranty & Remedy

AI Comment: The playbook item requires two elements: (1) a warranty that products and services perform materially in accordance with their documentation, and (2) a pro-rata refund if the vendor cannot repair or replace a non-conforming service. The QuickBooks Terms of Service materially conflict with both requirements.

ON WARRANTY: Section A's Disclaimers provision delivers the platform strictly on an "as-is" basis, expressly disclaiming all implied warranties including merchantability, fitness for a particular purpose, and non-infringement, and explicitly stating that Intuit does not warrant the platform's accuracy, reliability, or availability. There is no general warranty anywhere in the agreement that the platform performs in accordance with its documentation.

Narrow, conditional performance commitments do exist in Section B for specific sub-services: the Payroll Tax Accuracy Guarantee (Part F, §5.a) warrants timely, accurate payroll tax calculations and filings for Workforce subscribers, and the Accurate Books Guarantee (Part E, §6) commits to correcting bookkeeping errors at no charge. These fall short of the

acceptable position because: (a) they cover only specific sub-service categories, not the platform generally; (b) both are heavily conditioned on customer-side accuracy (correct/timely information, KYC clearance, sufficient funds); and (c) neither constitutes a warranty of conformance with Intuit's documentation.

ON REMEDY: The platform provides no pro-rata refund mechanism. Section A explicitly states "We do not provide refunds or credits for any cancellations or partial subscription period," and the Effect of Termination clause independently eliminates any refund entitlement upon termination. For the specific service categories that carry Section B performance commitments, the available remedies are even more narrowly capped: Part E, §7 limits Intuit's entire obligation for Live Expert Service errors to correcting the error in QuickBooks Online for the month the error occurred; Part F, §3.a limits Intuit's entire obligation for Payroll Payment errors to making the correct payment/filing and covering resulting tax penalties and interest. Both of these Section B provisions use "notwithstanding anything to the contrary in the Section A Terms" language, making them the exclusively governing remedial clauses for those services and foreclosing any broader recovery (e.g., under the general liability cap in Section A) that might otherwise apply.

SUPERSEDING EFFECT: Section B's explicit precedence clause ("These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms") together with the "notwithstanding anything to the contrary in Section A" language in Parts E.7 and F.3.a means the correction-only remedies in Section B are the controlling final remedies for Live Expert and Workforce/Payroll services respectively, replacing the general Section A as-is posture for those categories.

OVERALL: The contract's warranty and remedy structure materially conflicts with the acceptable position on both prongs. No warranty of conformance with documentation is provided for the platform; the sole available remedy for general platform issues is not refund but rather limitation of liability (§12 months fees or $100), and for specific services the remedy is expressly capped at correction-only. Since the item weight is "Acceptable to Deviate," the risk level is informational/noted rather than blocking, but the gap is clear and complete.

— Superseding reasoning —
Two superseding determinations apply within the Terms of Service. First, Part E, §7 (Live Expert Services Liabilities) uses explicit "notwithstanding anything to the contrary in the Section A Terms" language and is a Section B provision, which by the agreement's own precedence rule prevails over Section A. For Live Expert Service errors, the correction-only clause displaces the general Section A as-is disclaimer as the governing remedy provision. Second, Part F, §3.a (Payroll Payment Services) uses identical "notwithstanding anything to the contrary in the Section A Terms" language in Section B, and for Payroll Payment errors the correction/penalty-payment clause is the controlling remedial language rather than the general Section A as-is treatment. Neither superseding determination benefits the customer relative to the playbook item — both establish correction-only remedies that fall far short of the required pro-rata refund.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The only warranties we make about the Platform are (1) stated in this Agreement, or (2) as provided under applicable laws. The Platform is otherwise provided "as-is," and we do not make any other warr…"
2. "If you are a registered user of any Workforce Service, as long as the information you provide us is correct and on time and passes KYC Verification, and you have sufficient funds in Your Account, we'l…"

> *"We do not provide refunds or credits for any cancellations or partial subscription period."*
> — QBO Terms of Service for QuickBooks - US
> *"No expiration or termination will affect your obligation to pay all fees due or that may have accrued through the effective date of expiration or termination or entitle you to any refund."*
> — QBO Terms of Service for QuickBooks - US
> *"If the Bookkeepers made an error that requires re-opening of your books, we will correct the error for the month that error occurred at no additional charge."*
> — QBO Terms of Service for QuickBooks - US
> *"Notwithstanding anything to the contrary in the Section A Terms, if any Intuit error occurs in performing the QuickBooks Live Expert Services, our only responsibility will be to correct the error in QuickBooks Online for the month the error occurred."*
> — QBO Terms of Service for QuickBooks - US
> *"Notwithstanding anything to the contrary in the Section A Terms, if any Intuit error occurs in processing Payroll Payments, our only responsibility will be to make the correct payment or file the correct report and pay any resulting tax interest or penalty."*
> — QBO Terms of Service for QuickBooks - US

Encryption at Rest

AI Comment: The playbook item requires an explicit contractual commitment to encryption at rest using AES 256 bit or then-current industry standard. Across all five provided documents, no provision (i) expressly commits to encrypting data "at rest" as a distinct protection category, (ii) names AES 256 bit or any specific encryption algorithm, or (iii) imposes an unconditional obligation to encrypt data.

The controlling provisions are the QBO DPA §4.1 (governing Business Connection Data for general QuickBooks Online use) and the Time/Workforce DPA §2.5 (governing Customer Data for Workforce, Time, and Contractor Payments services). Both commit to implementing "appropriate technical and organisational measures" that "shall include, as appropriate" the "pseudonymisation or encryption of personal data." This language is materially weaker than the acceptable position for three compounding reasons:

1. Conditionality — Encryption is triggered only when deemed "appropriate" given factors including "costs of

implementation," granting Intuit contractual discretion to forgo encryption in certain circumstances.
2. Alternative pathway — "Pseudonymisation or encryption" permits substitution of pseudonymisation for encryption, meaning a full-encryption commitment is not mandatory.
3. No standard specified — Neither AES 256 nor any named cipher or key-length standard appears anywhere in the contractual documents; the DPA's reference to "state of the art" provides no enforceable floor.

The Privacy Statement's general "reasonable physical, technical and organizational safeguards" language (Doc 2) adds no specificity and is superseded for data-processing purposes by the express DPA hierarchy (QBO DPA §11.3, Time DPA application section). The Data Receipt Service's login-credential encryption commitment in the ToS (Doc 1 §D) is narrowly scoped to credential storage for one service function and does not address general data-at-rest protection.

This is classified YELLOW rather than RED because encryption is affirmatively addressed as a security measure within the DPA's mandatory measures list — it is not silence. However, the protection provided is materially and specifically weaker than the playbook's AES 256 at-rest requirement: the vendor retains full discretion over encryption depth, standard, and applicability. For a High-weight item, this warrants documented assessment and negotiation of explicit at-rest encryption language with a named standard.

— Superseding reasoning —
The QBO DPA (Doc 3) §11.3 establishes an explicit document hierarchy: "the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the Agreement," making the DPA's security provisions controlling over the ToS and the Privacy Statement for QBO data-processing security obligations. Similarly, the Time/Workforce DPA (Doc 4) application section states: "In the event of any discrepancies between the terms of this DPA and the Agreement with respect to the Processing of Customer Data, this DPA shall control." Accordingly, the QBO DPA §4.1 and Time DPA §2.5 security provisions each supersede the Privacy Statement's general safeguard language for contractual security purposes. The DPA security provisions are therefore the governing language against which the playbook item must be assessed. The ToS login-credential encryption clause (Doc 1 §D) is a narrow functional commitment addressing a single service feature and is not in conflict with the DPAs; no superseding relationship applies to it.

> *"At a minimum, Intuit shall implement appropriate technical and organisational measures to protect Business Connection Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures shall include, as appropriate:*
>
> *(a) the pseudonymisation or encryption of personal data;*
>
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
>
> *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*
>
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)
>
> *"Intuit shall implement appropriate technical and organizational measures to protect the Customer Data from a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."*
>
> — QuickBooks Time & Workforce (Time/Payroll) DPA
>
> *"We use reasonable physical, technical and organizational safeguards that are designed to protect your personal information."*
>
> — Global Privacy Statement | Intuit
>
> *"Maintained login credentials will be encrypted and used in connection with importing your data to our Service otherwise with your permission."*
>
> — QBO Terms of Service for QuickBooks - US

Breach Indemnification

AI Comment: The playbook requires indemnification from Intuit for (1) Intuit's own breaches and (2) breaches by subprocessors. Reviewing the full document set — Terms of Service (ToS), Global Privacy Statement, QBO DPA, and QB Time/Workforce DPA — the acceptable position is not met. This finding is RED for a HIGH weight item.

Intuit's Own Breaches — No Indemnification:
The ToS "Indemnity Obligations" section contains only a unilateral indemnification running from the customer to Intuit. There is no reciprocal clause under which Intuit would indemnify the customer for Intuit's own breaches. To the contrary, Intuit's total aggregate liability is capped at the greater of 12 months of fees or $100, with consequential, indirect, and incidental damages expressly excluded. Product-specific sections (payroll payments, Live Expert services) further narrow Intuit's remedy obligations to narrow make-whole remedies only (e.g., "our only responsibility will be to correct the error in QuickBooks Online for the month the error occurred").

Subprocessor Breaches — Partial Responsibility Language, Not Indemnification:
The DPAs do contain provisions acknowledging Intuit's responsibility for subprocessor compliance failures. The QBO DPA Section 3.2 states Intuit will "remain responsible" for subprocessor compliance failures, and the QB Time DPA Section 2.6 uses the stronger phrase "fully liable" for subprocessor breaches of the DPA clause. These are the closest provisions to the

playbook requirement. However, they fall materially short on three grounds: (a) they are framed as liability acknowledgments ("remain responsible," "fully liable"), not as indemnification obligations (no "indemnify, defend, hold harmless" language); (b) per QBO DPA Section 10.1, DPA liability is expressly tied back to the Agreement's liability exclusions and limitations — meaning the same 12-months/$100 cap and consequential-damage exclusions from the ToS apply; and (c) the QB Time DPA subprocessor provision covers only breaches of the DPA subprocessing clause specifically, not all subprocessor-caused breaches.

Positive Carve-Out — Narrow:
QBO DPA Section 10.3 provides that no party may limit its liability with respect to individual data protection rights. This carve-out prevents the Agreement's caps from applying to claims tied to individual data subject rights, which is a meaningful protection but narrow in scope — it does not constitute the full indemnification for all breaches that the playbook requires.

Superseding Determination:
For data processing matters, the DPAs control over the Agreement (QBO DPA Section 11.3; QB Time DPA Section 4.7). This means the subprocessor responsibility provisions in the DPAs govern, not the ToS indemnity section. However, the DPAs themselves tie their liability framework back to the Agreement caps (QBO DPA Section 10.1), except for individual data protection rights (QBO DPA Section 10.3).

Net Assessment:
The contract documents affirmatively exclude indemnification by Intuit for its own breaches, cap any liability at a commercially negligible level, exclude the damage categories most relevant to a financial data breach (lost data, revenues, profits), and frame subprocessor obligations as responsibility/liability acknowledgments rather than indemnification. This materially fails the acceptable position for a HIGH weight item.

— Superseding reasoning —
Two superseding determinations apply within this item. First, for data processing matters, the DPA subprocessor responsibility provisions (QBO DPA Section 3.2; QB Time DPA Section 2.6) supersede the ToS general indemnity section as the governing framework for breach liability related to data processing, because the DPAs sit above the Agreement in the contractual hierarchy (QBO DPA Section 11.3; QB Time DPA Section 4.7) and are more specific to data processing obligations. Second, within the QBO DPA, Section 10.3 (no party may limit liability for individual data protection rights) supersedes Section 10.1 (DPA liability subject to Agreement caps) for the specific category of individual data protection rights claims, as Section 10.3 is the more specific, targeted exception to the general cap rule in Section 10.1.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Business Connection Data as those…"
2. "Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liabi…"
3. "In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise."

> *"You will indemnify and hold harmless the Intuit Parties for any losses, damages, judgments, fines, costs and expenses (including legal fees) in connection with any claims arising out of or relating to your unlawful or unauthorized use of the Platform or violation of this Agreement."*
> — QBO Terms of Service for QuickBooks - US
> *"Limitation of Liability," "Indemnity Obligations," "Disputes," and "General Terms (Miscellaneous)"."*
> — QBO Terms of Service for QuickBooks - US
> *"Limitation of Liability," "Indemnity Obligations," "Disputes," and "General Terms (Miscellaneous)"."*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit remains fully liable for any breach of this Clause that is caused by an act, error or omission of its Subprocessor that is acting on our behalf under this DPA."*
> — QuickBooks Time & Workforce (Time/Payroll) DPA

Indemnification – Our Company to Vendor

AI Comment: The playbook requires that any customer indemnification obligation be limited to third-party claims arising from the customer's own content or misuse of the services; the ideal preference is no indemnification obligation at all.

Primary Clause (Section A): The general indemnification clause triggers upon "your unlawful or unauthorized use of the Platform or violation of this Agreement." The "unlawful or unauthorized use" language has partial conceptual overlap with the acceptable "misuse of services" standard. However, the additional phrase "violation of this Agreement" sweeps in any breach of the broader ToS — including payment failures, export control non-compliance, acceptable-use policy violations, and content restrictions — which significantly exceeds the acceptable scope. Additionally, Intuit reserves the unilateral right to assume "exclusive defense and control" of any indemnified claims (with costs borne by the customer), removing the customer's ability to manage its own exposure in indemnified disputes.

Section B Workforce/Payroll Clauses (directly relevant to stated use case — bookkeeping and payroll): The Workforce Services terms add indemnification obligations that are entirely outside the acceptable position:
- A broad obligation to indemnify for "any claims, liabilities, losses, and expenses … arising out of or related to your Plans, including Third-Party Partner Plans" (benefit plan administration) — with no nexus to content or service misuse.
- An obligation to indemnify for "any liability resulting from your failure to respond to [worker] requests for information" — entirely compliance-driven, not tied to content or misuse.

- Under QB Time, an obligation covering "(i) any and all payroll, tax, immigration and labor compliance liabilities" — well outside the acceptable scope — though part (ii) (Data Protection Law violations by the customer's use of Time) is closer to the acceptable "misuse" standard.

Messaging Services: A further provision imposes indemnification for claims arising from the customer's platform/ messaging use, and explicitly extends to "inquiries and investigations by local, state and federal regulators" — going beyond third-party civil claims to include regulatory proceedings, which exceeds the acceptable scope.

Section B Hierarchy Note: The Section B Product Specific Terms expressly prevail over Section A in any conflict. The obligations identified in Section B are additive (covering distinct scenarios rather than contradicting Section A) and thus all apply simultaneously, cumulatively broadening the customer's exposure.

Classification Rationale: YELLOW rather than RED because: (a) all indemnification obligations remain anchored to the customer's own conduct and actions (not arbitrary or one-sided as to liability for Intuit's own wrongdoing); (b) the primary Section A clause does partially overlap with the "misuse of services" standard in its "unlawful or unauthorized use" prong; and (c) the overall scope, while materially exceeding the acceptable position, does not constitute a complete contradiction of the underlying principle. However, the "violation of this Agreement" language and the numerous Section B obligations (payroll compliance, plan administration, worker information response failures) render the overall indemnification scope materially broader than the acceptable threshold. The ideal preference (no indemnification) is not met.

— Superseding reasoning —
The Section B Product Specific Terms expressly prevail over Section A General Terms in any direct conflict (per Section B introduction: "These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms"). However, the multiple indemnification provisions identified in this analysis are additive rather than conflicting — each applies to a distinct set of circumstances (general Agreement violations; benefit plan claims; worker information request failures; payroll/tax compliance liabilities; messaging service violations). All applicable clauses impose simultaneous, cumulative obligations on the customer. No superseding determination is required as between these provisions because they do not conflict with one another.

> *"You will indemnify and hold harmless the Intuit Parties for any losses, damages, judgments, fines, costs and expenses (including legal fees) in connection with any claims arising out of or relating to your unlawful or unauthorized use of the Platform or violation of this Agreement."*
> — QBO Terms of Service for QuickBooks - US
> *"Intuit reserves the right, in its sole discretion and at its own expense, to assume the exclusive defense and control of any claims."*
> — QBO Terms of Service for QuickBooks - US
> *"You agree to indemnify Intuit against any claims, liabilities, losses, and expenses (including legal fees), arising out of or related to your Plans, including Third-Party Partner Plans."*
> — QBO Terms of Service for QuickBooks - US
> *"You agree to indemnify and hold Intuit harmless from any liability resulting from your failure to respond to such requests for information."*
> — QBO Terms of Service for QuickBooks - US
> *"You agree to indemnify and hold Intuit harmless from (i) any and all payroll, tax, immigration and labor compliance liabilities and (ii) any liability arising from your or your Workers use of Time in a manner that violates Applicable Data Protection Laws"*
> — QBO Terms of Service for QuickBooks - US
> *"You also agree to indemnify and hold harmless Intuit from and against any claims, damages, losses, costs, or fees which may result from your use of the Platform, the Services, and/or Messaging Services, including, but not limited to, claims, damages, or lawsuits threatened or filed by third parties as well as inquiries and investigations by local, state and federal regulators (see Indemnity Obligations for additional responsibilities in this regard)."*
> — QBO Terms of Service for QuickBooks - US

License Grant – Vendor to Our Company

AI Comment: The playbook item requires that the license scope covers (1) intended use, (2) users, and (3) affiliates, with no restrictions that defeat the purpose of the purchase.

Intended Use — Covered (mitigated concern): QuickBooks Online is designed specifically for commercial business bookkeeping, income/expense tracking, payroll processing, and custom financial reporting — precisely the uses identified in the intake brief. Section A of the ToS limits platform access to "non-commercial purposes only," which on its face would be alarming for any business deploying the product commercially. However, the Section B Product Specific Terms contain an explicit prevailing clause ("These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms"), and Section B comprehensively describes commercial business services — payroll, tax filings, bookkeeping, invoicing, expense tracking, and financial reporting. Under standard superseding logic, the explicit Section B prevailing clause resolves the Section A conflict in favor of permitted commercial business use. Intended use is therefore covered.

Users — Conditionally Covered (subscription-gated): The Agreement permits the Administrator to authorize Additional Users on the same account, subject to limits set by the subscription tier purchased. This is a commercial tiering model, not an absolute prohibition: the customer can select a plan that accommodates its required user count. This restriction does not defeat the purpose of the purchase, though it should be verified that the selected subscription tier is compatible with the organization's intended user population.

Affiliates — Not Covered (material gap): This is the decisive deficiency against the playbook requirement. The software license is expressly "personal, limited, nonexclusive, nontransferable, and revocable," and the platform access right is

scoped to "your own internal" use only. The Assignment clause prohibits transfer of rights to any third party — including affiliates — without Intuit's prior written consent. There is no affiliate extension clause, no multi-entity or enterprise affiliate provision, and no language permitting related legal entities to operate under a single customer subscription. Each affiliated legal entity requiring access would need a separate QuickBooks account and subscription. For organizations with subsidiaries or commonly controlled affiliates that need to use QuickBooks for their own bookkeeping or payroll, this is a material limitation.

Additional License Risk Factors: The software license is revocable, and Intuit retains a unilateral right to "modify, suspend or discontinue the Platform at any time" without liability. These terms are common in SaaS contracts but create continuity risk that reviewers should weigh.

Overall: YELLOW — the license satisfactorily covers the stated commercial intended use (via Section B prevailing) and permits users within subscription tiers, but it does not extend to affiliates. The acceptable position in the playbook is only partially met. The affiliate gap is the controlling issue for this classification. For organizations with multiple legal entities, this requires either negotiation for an affiliate extension or procurement of separate per-entity subscriptions.

— Superseding reasoning —
Section A of the ToS restricts platform access to "non-commercial purposes only." Section B contains an explicit provision stating the Section B Terms prevail over any conflict or inconsistency with Section A. Because Section B describes commercial business services (payroll, bookkeeping, financial reporting), the "non-commercial" restriction in Section A conflicts with and is superseded by the Section B terms for QuickBooks users. PIF[1] (Section B prevailing clause) supersedes PIF[0] (Section A non-commercial restriction). The governing language for permitted use is therefore the Section B commercial business service framework, not the Section A non-commercial limitation.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Your use of the Services provided by Intuit (as defined in the Section A Terms) and described below are subject to the Section A Terms above and these Additional Terms and Conditions ("Section B Terms…"
2. "Conditioned upon your compliance with the terms and conditions of this Agreement (including all payment obligations), Intuit grants you a personal, limited, nonexclusive, nontransferable, revocable li…"
3. "Administrators may authorize additional users to access the applicable Services through the same account, subject to limitations based on the subscription you purchase (such users, "Additional Users")…"

> *"Except as set forth in the Section B terms, you may access and use the Platform for your own internal, lawful and non-commercial purposes only."*
> — QBO Terms of Service for QuickBooks - US
>
> *"We may limit usage for some features of the Services that require a subscription based upon the subscription you purchased. These features may include chart of accounts, classes and locations (combined), system-generated fields, third party applications, and users."*
> — QBO Terms of Service for QuickBooks - US
>
> *"Intuit may assign or transfer this Agreement to any party at any time without notice to you. You may not assign your rights under this Agreement, by operation of law or otherwise, without our consent. Any attempts to do so without our consent will be void."*
> — QBO Terms of Service for QuickBooks - US
>
> *"We may further modify, suspend or discontinue the Platform at any time. You agree that we will not be liable to you or any third party for any modification, suspensions, or discontinuance of the Platform."*
> — QBO Terms of Service for QuickBooks - US

Employee Confidentiality Agreements

AI Comment: The playbook requires that vendor employees who access data enter into **written** confidentiality agreements. The document set addresses confidentiality obligations for authorized personnel in two separate DPAs, but both fall short of the acceptable position by explicitly permitting non-written alternatives.

DPA Doc 3 (QBO) — Section 4.2 requires authorized persons to be under "an appropriate obligation of confidentiality (whether a contractual or statutory duty)." The disjunctive "or statutory duty" language means Intuit can satisfy this obligation through applicable law alone, without a written, individually-executed agreement. A statutory duty (e.g., general employment law confidentiality implied by California or federal law) is meaningfully different from a purpose-specific written agreement that personally binds each employee to defined obligations regarding customer data.

DPA Doc 4 (Time/Workforce) — Section 2.4 is even broader: it allows satisfaction through "a duty under internal policy, contractual duty or a statutory duty." The addition of "internal policy" as an acceptable mechanism means Intuit could rely on a general employee handbook or company-wide policy rather than individual written agreements — a materially weaker protection.

Neither DPA requires that the confidentiality obligation take the form of a **written agreement** entered into by each person who accesses data. The acceptable position under the playbook is that written agreements must exist. The vendor's terms address the same topic (confidentiality of data by personnel) but with structurally weaker and more permissive language. This is a YELLOW finding under the functional-equivalence standard: the same topic is addressed, but the protection is narrower in scope and enforceability.

The ToS (Doc 1) contains no independent employee confidentiality provision. Per DPA 3 §11.3 and DPA 4 §4.7, both DPAs take precedence over the ToS on data-processing matters. As the two DPAs cover distinct service scopes (QBO vs. Time/

Workforce), both findings remain independently operative and are not superseded by one another.

— Superseding reasoning —
No superseding determination applies between PIF 1 and PIF 2. The QBO DPA (Doc 3) governs Business Connection Data processed under the QuickBooks Online subscription; the Time/Workforce DPA (Doc 4) governs Customer Data processed under Time, Workforce, and Contractor Payments services. These are parallel instruments with independent scope, not conflicting provisions addressing the same data set. Both DPA documents expressly take precedence over the ToS on data-processing matters (DPA 3 §11.3; DPA 4 §4.7), and the ToS contains no employee confidentiality language that competes with either DPA provision.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall ensure that any person that it authorizes to Process the Customer Data (including Intuit's staff, agents and subcontractors) (an "Authorized Person") shall be subject to a strict duty of …"

> *"Intuit shall ensure that any person who is authorized by Intuit to process Business Connection Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty)."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Restrictions on Use

AI Comment: This item requires that vendor use restrictions not prohibit the intended use of QuickBooks for bookkeeping, income/expense tracking, payroll processing, and financial report generation, with only standard acceptable-use restrictions being acceptable. The preference is no restrictions beyond a minimal standard AUP.

Section A General Use Grant vs. Section B Commercial Use (Superseding Analysis): The Terms of Service operate on a two-tier structure. Section A establishes a general baseline — users may access the Platform "for your own internal, lawful and non-commercial purposes only." Standing alone, the "non-commercial" qualifier could be read to limit commercial business use (bookkeeping, payroll, and financial reporting all occur in a commercial context). However, Section A expressly carves out Section B ("Except as set forth in the Section B terms"), and the Section B introduction contains an explicit precedence clause: "These Section B Terms will prevail over any conflict or inconsistency with the Section A Terms." Section B Product Specific Terms describe and enable exactly the intended commercial business functions — payroll processing, bookkeeping, financial reporting — as core QuickBooks product use cases. After superseding logic is applied (PIF[1] supersedes PIF[0]), the governing position is that commercial QuickBooks business use is fully permitted. The Section A "non-commercial" tension is resolved by the express hierarchy provisions.

Standard Prohibited Uses (Section A): The Prohibited Uses list is substantially standard AUP content — prohibitions on illegal activity, IP infringement, spam, unauthorized access, reverse engineering, impersonation, and resale. None of these items conflict with the intended bookkeeping/payroll/financial reporting use. One item warrants specific notation: the prohibition on "training or developing artificial intelligence or machine learning models or related technology using information derived from the Platform without authorization" is an emerging SaaS restriction type increasingly seen in post-2023 vendor agreements. While it does not impair the core intended use, it represents a restriction that goes beyond legacy standard AUP text and could constrain future data-analytics or AI-augmented use of QuickBooks data exports. Additionally, "Use the Platform for general archiving or back-up purposes" is prohibited — not relevant to the intended use. Both are the reason aiPreferenceMet is false.

Workforce Geographic Restriction (Section B, Part F): Payroll and Workforce Services are expressly limited to use in the United States and only with US-based workers. This does not impair the intake context (US SaaS deployment) but represents a product-specific limitation that goes beyond a generic AUP.

Acceptable Use Policy — Payment / Money Movement Services (Document 6): The AUP for money movement services enumerates a detailed table of prohibited merchant/business types. These restrictions are standard for a licensed money transmitter and reflect card network and sponsor bank compliance obligations rather than general software use restrictions. Notably, "Financial Institutions and Regulated Financial Products, Services and Securities including Payment Facilitators and Money Service Businesses" is listed as prohibited for both payroll/direct deposit AND merchant payment processing. If the reviewing organization is itself a financial institution, this restriction would materially impair payroll processing via QuickBooks. The intake brief describes a standard bookkeeping/payroll user with no indication of a prohibited business type affiliation; accordingly, this restriction is not presently triggered but should be confirmed by the reviewing legal team.

Overall Assessment: Classification is GREEN — the restrictions present do not prohibit the intended use of bookkeeping, expense tracking, payroll, and financial reporting. The restrictions are standard or near-standard for a SaaS financial platform. The acceptable position ("must not prohibit our intended use; standard acceptable-use restrictions are acceptable") is met. The preference of "no restrictions beyond a standard acceptable-use policy" is not fully met (aiPreferenceMet=false) because: (1) the AI/ML training prohibition is a newer restriction class not present in legacy standard AUPs; (2) the payment services AUP is a detailed financial-services regulatory compliance document — significantly more extensive than a generic software AUP; and (3) the geographic restriction on payroll services adds specificity beyond a generic AUP. None of these impair the intended use, and all reflect standard industry practice for financial technology platforms.

Action recommended for human reviewer: Confirm that the reviewing organization does not fall within a prohibited business type category under the payment AUP (particularly the financial institution / money service business restriction),

which would impair payroll processing services.

— Superseding reasoning —
Section A of the Intuit Terms of Service imposes a general Platform use baseline of "internal, lawful and non-commercial purposes only" — language that in isolation conflicts with commercial bookkeeping/payroll use. However, Section A itself carves out Section B ("Except as set forth in the Section B terms"), and the Section B introduction contains an express precedence clause stating that Section B Terms "will prevail over any conflict or inconsistency with the Section A Terms." Section B Product Specific Terms for QuickBooks explicitly describe and enable commercial business functions (payroll, bookkeeping, financial reporting). Applying the SPECIFIC_OVER_GENERAL principle, the QuickBooks-specific Section B terms govern over the general Platform Section A baseline. The governing language permits commercial business use through QuickBooks services.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Your use of the Services provided by Intuit (as defined in the Section A Terms) and described below are subject to the Section A Terms above and these Additional Terms and Conditions ("Section B Terms…"
2. "Intuit does not condone or support any activity that is illegal, violates the rights of others, harms or damages Intuit's reputation, or could cause Intuit to be liable to a third party. At minimum, y…"
3. "You may only use Workforce Services (i) in the United States and (ii) solely with respect to employees and contractors ("Workers") located in the United States."

> *"Except as set forth in the Section B terms, you may access and use the Platform for your own internal, lawful and non-commercial purposes only."*
> — QBO Terms of Service for QuickBooks - US
> *"Prohibited Uses, Transactions and Prohibited/Restricted Business Types or Activities.** In addition to the [Intuit Terms of Service](https://www.intuit.com/legal/terms/), if any of the following apply, you are ineligible (or may become ineligible) to use our Services, and we may take any corrective action that we deem appropriate:"*
> — Acceptable Use Policy (payments / money movement)

Compliance Monitoring

AI Comment: The playbook item requires the vendor to proactively and periodically — at minimum annually — review its own compliance with the DPA and applicable data protection and privacy laws, and to adapt where necessary. This is a vendor self-assessment obligation, not a customer audit right.

Across all five substantive documents (Terms of Service, Global Privacy Statement, QBO DPA, Time/Workforce DPA, and Telecom Terms), no provision explicitly commits Intuit to an annual — or any other defined-cadence — compliance self-review against the DPA or applicable data protection laws.

Three partial provisions are cited as PIFs:

1. **QBO DPA § 4.3 (Updates to Security Measures):** Intuit commits to updating security measures "from time to time," subject to a non-degradation floor. While this reflects an ongoing adaptation posture, "from time to time" is materially weaker than "at least annually" — it could occur more or less frequently with no accountable cycle. This does not satisfy the annual review cadence required by the playbook item.

2. **QBO DPA § 5 (Security Reports and Audits):** Intuit makes security audit reports available for customer review and allows written compliance questions. This is a customer-triggered mechanism — it places the compliance verification burden on the subscriber rather than establishing a vendor self-review obligation. It is directionally useful but does not meet the standard.

3. **Time/Workforce DPA § 2.11 (Audit):** Intuit agrees to respond to written audit questions no more than once per year. Again, this is customer-initiated and limited to Intuit's security practices — not a holistic DPA/privacy law compliance review by Intuit itself. The "no more than once per year" cap also frames this as a ceiling on customer requests rather than a floor on vendor action.

None of these provisions satisfy the playbook requirement because: (a) they lack a defined annual cycle tied to vendor self-assessment; (b) those that reference an annual cadence are framed as customer rights, not vendor obligations; and (c) the "from time to time" language provides no accountability for compliance gaps that may persist between unscheduled updates. Given the context — QuickBooks processing sensitive bookkeeping, payroll, and financial data for an organization's business operations — the absence of a defined vendor compliance review cycle is a material gap. Classification is RED at High weight, with no applicable statutory or industry-norm downgrade justifying relief.

— Superseding reasoning —
No superseding determination is required among the three cited PIFs. The QBO DPA (Doc 3) and the Time/Workforce DPA (Doc 4) address different service scopes (general QuickBooks Online vs. Time/Workforce services respectively) and are additive rather than conflicting on this topic. The QBO DPA's own hierarchy clause (§ 11.3) establishes that the DPA prevails over the general Agreement for data processing matters, but this hierarchy does not resolve the absence of an annual review commitment — it only confirms the DPA is the controlling instrument. No document-level conflict exists that requires a superseding resolution for this item.

— Note —

The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Intuit shall make available reasonably necessary information to demonstrate compliance with the obligations laid down in this DPA. In particular, Intuit allows Customer to review security audit report…"
2. "Intuit shall respond to any written audit questions related to Intuit's security practices submitted to it by Customer, provided that Customer shall not exercise this right more than once per year."

> *"Customer acknowledges that the Security Measures are subject to technical progress and development and that Intuit may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Customer."*
> — DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)

Documents

Title	URL	Type	Scraped At	Replaced
QBO Terms of Service for QuickBooks - US	https://intuit.com/legal/terms/en-us/quickbooks/online	text/markdown	2026-07-14T11:38:28.051Z	No
Global Privacy Statement | Intuit	https://intuit.com/privacy/statement	text/markdown	2026-07-14T11:39:18.371Z	No
DPA - QuickBooks Online Data Processing Agreement - US and Canada (Please reference #25164 before editing)	https://intuit.com/legal/terms/en-us/quickbooks/qbo-data-processing	text/markdown	2026-07-14T11:42:19.887Z	No
QuickBooks Time & Workforce (Time/Payroll) DPA	https://intuit.com/legal/terms/en-us/quickbooks/time-payroll-data-processing	text/markdown	2026-08-09T11:51:51.709Z	No
Intuit Telecom Specific Terms	https://intuit.com/legal/terms/en-us/other/telecom	text/markdown	2026-08-09T11:52:32.538Z	No
Acceptable Use Policy (payments / money movement)	https://quickbooks.intuit.com/payments/legal/TOC102017/acceptable-use	text/markdown	2026-08-09T11:53:15.713Z	No

Beyond-Playbook Findings

None.

Reviewers

Name	Current Step
Acme Tenant Admin	ANALYSIS