Compliance Company Research

COMPANY #1: CLEARWATER

Clearwater -https://clearwatersecurity.com/ Company overview Services offered HIPAA/security/compliance capabilities SOC 2 / HITRUST / ISO certifications supported Audit readiness support External auditing services Startup-friendly offerings Estimated pricing ranges (focus on cost-effective options) Advantages/disadvantages for Wenixo's current stage Whether services are more appropriate for: a. early-stage startups b. scaling startups c. enterprise healthcare systems	1. Company Overview d. Founded in 2009. Build a comprehensive set of solutions that avoid preventable breaches, optimize security investments, and effectively meet compliance requirements. e. Combines deep healthcare security and compliance expertise with MSSP capabilities, managed cloud services, consulting and assessments, and compliance software. f. Over 650 customers using the managed services, consulting services, and IRM|Pro software. g. Named the top Compliance and Risk Management solution provider in Black Book Market Research's annual survey of the healthcare industry the past 8 years in a row. Top rated Cybersecurity Advisors and Consultants for the last 5 years. 2. Services Offered: a. To Digital Health Companies: firewall management, continual threat detection, attack monitoring, incident response. b. ClearAdvantage Program: Help develop strategic and tactical roadmaps. Combines the cybersecurity and compliance components that align with the NIST Cybersecurity framework. 3. HIPAA/security/compliance capabilities a. Team of former regulators, lawyers, and cybersecurity leaders. b. HIPAA Risk Assessments, expert support during OCR enforcement, audits, and investigations.

	c. HIPAA Risk Analysis: OCR-Quality Risk Analysis Solution evaluates threats and vulnerabilities to all information systems used to receive, create, transmit, or store ePHI, while also complying with the strict guidance from OCR. i. Assess policies and Procedures, Assess infrastructure, Physical walkthroughs, inventory systems with ePHI, Assess systems and components with ePHI, tech enables, structured data repository, AI, on-demand reporting, risk response, risk management, remediation optimization, remediation support, single, centralized risk register, peer-to-peer reporting, consistent year-over-year reporting, meets OCR requirements, OCR support included, ongoing advisory services d. HIPAA Security Assessment: Security gap assessment is expert-led and supported by their industry leading IRM|Security software solution. Hands-on assessment workshop, conducted following OCR audit protocols. i. Education to help staff maintain compliance status and to perform and document this evaluation yearly, as the HIPAA security rule mandates. Evaluation of HIPAA security rule compliance. Fully documented assessment data, along with all related details populated in IRM|Security SaaS software. Training for privacy and breach notification compliance team on how to utilize Clearwater IRM|Security software to facilitate remediation tasks and perform future HIPAA Security Rule compliance assessments e. NIST Privacy Framework i. HIPAA Privacy and Breach Notification assessment helps identify any obligation issues in following the letter of the law and OCR audit protocols. Powered by IRM|

Privacy software solution, hands on training and assessment workshop evaluates compliance gaps and maturity.

f. Related HIPAA Security and Support Services:
    i. 10 point Assessment: Find where the company stands and get a clear action plan with a rapid 10 point tactical assessment of current HIPAA Compliance and cyber risk management process. Report includes actionable recommendations to address any identified gaps.
    ii. Policies and Procedures: A complete set of HIPAA Policy and procedure templates developed by experts to satisfy the strict requirements of the regulations that then are customized for our organization so they are aligned with Wenixo's operations and needs
    iii. Technical Testing: Security experts combine "cutting-edge" tools, comprehensive manual testing, and unparalleled real world technology experience to improve your overall security posture through vulnerability and penetration testing services.
    iv. Workforce Training (previously mentioned): Proven web-based program effectively addresses HIPAA mandates for workforce's security awareness and privacy training.

4. SOC 2 / HITRUST / ISO certifications supported
    a. SOC 2 ✅: Covers: Security policies and procedures, security governance structure and board reporting, risk analysis and risk response, technical testing and vulnerability scanning, penetration testing, strategic planning, security awareness training, secure architecture review, security breach response, cyber insurance policy review, buisness continuity planning and testing,

	disaster recovery planning and testing, vendor risk management b. Hitrust ✅: i. 1 year (e1) Validated Assessment: Designated to cover foundational cybersecurity practices for lower risk healthcare covered entities and business associates. This validated assessment leverages a leaner set of controls, making it ideal for smaller organizations and startups looking to differentiate themselves in the marketplace. ii. Risk-Based, 2 year (r2) Validated Assessment: Assessments performed against HITRUST CSF look at the various in-scope control and their maturity scores for Policy, Procedure, Implemented, Measured, and Managed categories. Can lead to HITRUST certifications based on achieving an appropriate overall assessment score. Help identify the actions needed to ensure a high maturity rating and achievement of HITRUST CSF r2 Certification iii. Implemented, 1-year (i1) Validated Assessment: Designated for healthcare covered entities and business associates that need moderate assurance, this 1-year certification focuses on a list of controls designated and updated yearly by HITRUST, implemented maturity is tested by these controls. Assessors will review, validate, and submit the assessment to HITRUST for approval. iv. Interim Assessment: Must be completed at the 1 year mark from certification as required by HITRUST for 2 year validated assessments. This determines if the controls in palace are still effective as well as evaluates progress against any Corrective

	Action plans that were created during the initial validation process. c. Certifications: i. PCI DSS ii. DEA-EPCS iii. CMMC d. Privacy Risk Assessment: i. State Data Privacy Law Assessment ii. GLBA iii. NIST Privacy Framework iv. 42 CFR Part 2 v. Privacy in Research vi. Information Blocking e. Program Development Components i. Tailored Privacy Framework ii. Policy and Procedure Development iii. Privacy Program Gap Assessment iv. Incident Response Planning v. Ongoing Program Maturity Support vi. Governance Structure Design 5. Audit readiness support a. Clearwater Security provides cybersecurity, risk management, and compliance services that help healthcare and health-tech companies prepare for and pass security audits and certifications (SOC 2, HITRUST, HIPAA). i. Gap assessments, Control implementation guidance, Audit preparation support, Certification readiness, Prepare for HITRUST certification, Implement required controls, Get ready for external assessors 6. External auditing services a. HITRUST b. PCI DSS c. SOC 2 d. CMMC e. EPCS 7. Startup-friendly offerings

	a. The SOC 2/HITRUST readiness support audit prep includes gap assessments, help identify missing controls, builds a compliance roadman, and has audit readiness guidance. This is startup friendly because Wenixo does not need a fully internal security team yet and helps get through enterprise vendor reviews, which is crucial for early sales b. HIPAA Compliance Programs. We get risk analysis, policies and documentation support, security gap identification and remediation planning. This is useful for Wenixo because it is required for any health data handling startup and helps pass procurement/security questionnaires from hospitals c. The Digital health tailored program can help Wenixo look enterprise ready very early on in the company's history. 8. Estimated pricing ranges (focus on cost-effective options) a. I am not aware of the company's financial situation, however given the recent genesis of the company, I presume cheap is the name of the game. This company does not have specific pricing available on their website but given other research this is what should be expected: i. Risk Assessment: $15,000+ ii. SOC 2 Readiness $20,000+ iii. HITRUST Readiness $40,000+ iv. Managed Compliance $3,000 - $15,000/Month 9. Advantages/disadvantages for Wenixo's current stage a. Advantages: i. Fast path to enterprise readiness. Meeting requirements for HIPAA, SOC 2, HITRUST ii. Strong credibility with healthcare buyers iii. vCISO level expertise without the hire iv. Helps pass security questionnaires faster. Can help Wenixo respond correctly early, avoid back and forth delays and reduce deal friction

	b. Disadvantages: i. Expensive. A lot of good programs can be purchased on the cheaper end here including the HITRUST e1 Assessment, but a lot of the other programs are not meant for early-stage startups. ii. Consultant driven, less automation iii. The full enterprise approach might be more than necessary for a growing company 10. Whether services are more appropriate for: enterprise healthcare systems a. This is meant for enterprise healthcare systems but has some programs Wenixo can benefit from at a smaller price. The company is reliable and trustworthy and might be a better go to than a newer unproven company.

COMPANY #2 DRATA

Drata - https://drata.com/ Company overview Services offered HIPAA/security/compliance capabilities SOC 2 / HITRUST / ISO certifications supported Audit readiness support External auditing services Startup-friendly offerings Estimated pricing ranges (focus on cost-effective options) Advantages/disadvantages for Wenixo's current stage	1. Company Overview: a. Drata is a global operation with offices in San Francisco, New York, London, and Sydney. But despite being worldwide, they are a great fit for startups looking to nail initial compliance procedures. Founded by former NASA operators, their company now reaches over 8 thousand clients, supports over 30 frameworks, has 3 thousand plus trust centers created and 15.7 Million evidence items processed daily. 2. Services Offered a. The Agentic Trust Management Platform: i. Agentic TPRM Assessment: AI autonomously retrieves vendor documents, evaluates it using centralized criteria, and highlights areas that require attention. The agent then generates targeted follow-up questions based on criteria gaps and communicates directly with the vendor. Upon completion, the agents produces assessment outputs that link criteria, evidence, and conclusions in one place. ii. AI Questionnaire Assistance: AI answers security questionnaires using external Trust Center content and Internal Knowledge Base documentation to reduce manual work and

Whether services are more appropriate for: a. early-stage startups b. scaling startups c. enterprise healthcare systems	accelerate sales cycles. Utilizing approved security and compliance information, AI can quickly generate accurate responses when new questionnaires are submitted while continuously learning based on human approvals and edits. iii. AI policy-to-control mapping: As new policies are approved or published, AI suggests accurate control mappings from policy text, cutting setup time and improving framework alignment. AI analyzes the content and surfaces the controls most likely to apply, then provides recommended mapping to ensure completeness, traceability, and strong audit readiness iv. Key Features: 1. AI Vendor SOC 2 summaries: Ai extracts key insights from SOC 2 reports to streamline third-party assessments and save teams valuable time. 2. AI Vendor Questionnaire summaries. AI highlights critical compliance details from vendor questionnaires to third party risk assessments 3. AI Test failure Insights: AI explains test failures to help teams understand issues quickly and remediate compliance gaps. 4. AI Trust Library Search: AI searches the Trust Library to help GRC teams find content instantly, answer questions faster, and accelerate customer reviews. 5. AI Chrome Extension: AI assists directly in customer trust portals, filling out questionnaire answers without switching tabs or losing context. 6. AI-generated Cloud Tests: Builds automated tests for AWS, Azure, and GCP to expand coverage and boost control assurance. 7. AI Document Parsing: Extracts questions from PDFs and DOCX files to accelerate questionnaire completion

	and reduce manual effort. 8. AI Trust item descriptions: Ai generates high-quality, externally-facing Trust item descriptions in seconds for faster onboarding and more consistency. 9. AI Suggestions for Policy Center: Provides control suggestions for custom and modified policies to extend audit readiness and reduce manual oversight. 10. AI Search for Collaboration Tools: Provides answers to trust questions asked via slack and microsoft teams. 11. AI Knowledge Base Management: Automatically identifies invalid entries, questions, answers and conflicting answers in your knowledge Base. b. Enterprise GRC i. Centralize Documentation in a Unified Platform: Consolidates control requirements, policies, evidence sources, ownership, and workflows into a single system of record so programs scale consistently across regions, teams, and frameworks. ii. Standardize Evidence Across Compliance Frameworks: Enterprise GRC utilizes native AI features to centralize evidence, control mappings, and audit workflows in one system of record so you can reuse what's already been validated, generate consistent audit-ready outputs, and run faster audits with fewer interruptions. iii. Establish Clear Accountability Across Ever Control: Assigns accountable owners to controls, risks, and evidence with standardized workflows and escalation paths, so issues route to the right teams fast, progress is trackable and remediation stays on schedule across business units. iv. Report Real-Time Posture with Confidence: Real time view of control statues and ownership across frameworks and business units so leadership can track trends, prioritize risk, and report posture with confidence

year-round.

v. Features:
    1. Policy and Personnel Management
    2. User Access reviews
    3. Custom workflows
    4. Enterprise grade workspaces
    5. Internal risk management
    6. Vendor risk management
    7. Vulnerability and asset management
    8. Multi-framework support
    9. Controls and evidence
    10. Monitoring and tests
    11. Compliance as code

c. Compliance Automation:
    i. Replace Manual Tracking with Continuous Automation: Centralizes controls and evidence in one place and automates collection across tools so compliance programs stays current as the team grows and tech stack changes.
        1. Assign ownership to controls and evidence
        2. Centralize and reuse evidence across audits: Store, manage, and reuse evidence artifacts with the centralized evidence library. Evidence lives on one system of record, linked once and reused across frameworks and audits, to help teams avoid re-uploading artifacts, reduce version confusion, and respond to audit requests with confidence.
    ii. Audit Prep: Continuously collects evidence and maintains control status over time, so audits are faster, calmer, and more predictable.
        1. Run continuous control tests across the environment.
        2. Extend monitoring and custom tests and connections: Teams define custom test logic and map results directly to controls in scope. Tests run on a recurring basis and surface outcomes alongside native checks, allowing enterprises to monitor critical controls consistently across all systems.
        3. Clear control ownership: ownership remains visible alongside control status

	and history. Teams can track recurring issues, follow up with the right stakeholders, and show auditors that controls are actively overseen. 4. Prove performance during audits and reviews: Instead of recreating context each audit cycle, teams can demonstrate consistent oversight and repeatable control performance. This reduces audit prep, limits back-and-forth, and gives confidence in the program's accuracy. iii. Assign Owners and Close Gaps faster: Compliance automation assigns control owners and routes remediation to the right people with clear tracking so risks get resolved quickly and accountability stays lightweight. iv. Accurate Reporting is difficult… See readiness in real time: Compliance automation provides a real time view of control health and evidence coverage so you can prioritize confidently and report readiness without guesswork. d. Trust Center: i. Remove Friction from the buying process: Gives prospects and customers a self-serve portal for security information and a designation access request process so reviews move faster without constant coordination. ii. Control and Manage content in a singular location: Uses structured access requests, approvals, and permissioning so sensitive documents are shared deliberately, consistently, and traceably. iii. Centralize Trust Posture: Organizes your trust library into a single destination buyers can navigate to answer their own questions so no one is manually creating the same responses for every prospect. iv. Answer faster with reusable, approved responses: Trust Center includes a trust library with reusable, consistent responses to reduce repetitive requests and works natively with AI Questionnaire Assistance to provide immediate responses. v. Features:

	1. Access Requests and Approvals 2. Trust Library 3. Document Sharing Controls 4. Searchable Buyer Experience 5. Brandable and Easy to Maintain 6. Trust Measurement e. AI Questionnaire Assistance i. Streamline Questionnaire Management at Scale: Centralizes how teams manage, track, and collaborate on inbound security questionnaires so nothing gets lost, delayed, or duplicated. Real time visibility into task owners, statuses, and deadlines, simplify complex workflows and complete questionnaires faster ii. Leverage AI to automatically generate responses: SMEs input answers to common questions into the knowledge base and upload relevant documentation to the trust center. The AI then utilizes this approved security and compliance information to quickly generate accurate responses when new questionnaires are added iii. Keep complete control with Humans in the Loop iv. Continuous Learning: Analytics dashboards show AI accuracy, AI completion rate, total number of responses generated, and more to highlight how effectively AI is supporting questionnaire workflows and enable quick remediation if analytics tend downward. v. Features: 1. Hassle free formatting 2. Integrated trust center 3. Automated analysis 4. Dynamic integrations 5. Full human review 6. Powerful analytics f. Third Party Risk Management: i. Drata helps teams collect vendor documentation, evaluate it against context aware risk criteria, and flag necessary follow ups. With a central place to track vendors and associated risks, teams can understand their third-party risk posture at any time. ii. Manage all third party risk in a centralized

	location: Document identified third party risks, such as when a vendor lacks required controls, does not complete penetration testing, or has red flags in their SOC 2 report. iii. Monitor Risk continuously and proactively iv. Collect documents, flag gaps, and follow up with agentic AI: Agent collects vendor documents, evaluates them against defined criteria, highlights gaps, and facilitates follow up questions. v. Features: 1. AI criteria generation 2. Vendor source sync 3. Ai risk summaries 4. Risk register 5. Third party directory 6. Executive reporting 3. HIPAA/security/compliance capabilities a. HIPAA: i. Eliminate Redundant HIPAA Preparation: Drata reuses shared controls and evidence across frameworks, reducing repeated documentation work. Teams maintain defensible records for audits, investigations, and internal reviews without rebuilding evidence each time oversight cycles repeat or scope expands. 1. Define controls once across frameworks: Input and manage controls in a single location so teams can stay aligned. Controls are written once and automatically mapped across frameworks, allowing teams to scale compliance programs as requirements change without rewriting controls or rebuilding audit foundations. 2. Assign ownership to controls and evidence 3. Centralize and reuse evidence across audits and stay audit ready with continuous visibility. ii. Track PHI risk across security and privacy: Drata links HIPAA related risks directly to safeguards, controls, and evidence to give teams a consistent and current view of exposure

	1. Centralize risks and automate control mapping: Document internal risks in a consistent, auditable way with a centralized risk register. You can start with a pre-mapped library of 200+ common risks or create custom risks to reflect your environment, so teams agree on what the risk is before determining ownership, impact, or treatment plans. 2. Assess and prioritize risk exposure: Capturing the likelihood and impact using configurable fields and formulas that match how your organization evaluates exposure. Risks are prioritized based on real context. 3. Plan and track risk assessment. You can assign remediation tasks natively or create Jira tickets so ownership is clear and progress is tracked. 4. Maintain Continuous Risk Visibility 5. Tools: a. Identify risk scenarios b. Analyze current risk c. View risk posture d. Determine treatment e. Implement treatment plans f. Assign ownership iii. Clarify HIPAA Control Gaps During Reviews: Uses AI to explain control test issues tied to HIPAA security and privacy requirements, including when controls behave unexpectedly. iv. Prepare for assessments without disruption: Centralizes evidence, testing results, and auditor collaboration so teams prepare for recurring HIPAA assessments more predictably. Reviews become less disruptive as documentation, ownership, and responses stay organized between assessment cycles. v. Additional Capabilities: 1. Utilize safeguards 2. Monitor safeguard controls 3. Track compliance risks 4. Oversee policies 5. Retain audit evidence 6. Review business associates

	4. SOC 2 / HITRUST / ISO certifications supported a. SOC 2 b. ISO 27001 c. GDPR d. HIPAA e. CMMC f. PCI DSS g. FedRAMP h. HITRUST i. TISAX j. NIST AI RMF k. NIS 2 l. CCM m. CIS n. CCPA o. Cyber Essentials p. DORA q. Essential Eight r. ISO 27701 s. ISO 27017 t. ISO 27018 u. ISO 42001 v. Microsoft SSPA w. NIST 800-171 x. NIST 800-53 y. NIST CSF 2.0 z. NYDFS aa. FFIEC bb. COBIT cc. SOX ITGC dd. FedRAMP 20x ee. Custom Frameworks 5. Audit readiness support: a. Consolidating messages, tasks, and evidence into a secure portal so nothing gets lost and timelines stay clear. b. Communicate with your auditor on the platform, track approvals, and understand expectations so you can close audits faster. Auditors can pick sample data and request documents. Drata automatically pulls in the

	evidence of the audit period to the hub, eliminating endless emails, Slacks, and notifications requesting evidence. Within the portal itself, auditors can view past audits for added context and better understanding of the current one. c. Drata works with a curated network of enterprise-grade audit firms in the Auditor Alliance to deliver consistent, defensible audit outcomes. d. Features: i. Add your auditors ii. Download packages iii. View auditor requests iv. Communicate effectively 1. Upload additional evidence, update the status, or respond to questions from the auditor in threat to track discussions v. Freeze and finalize vi. Run internal audits 6. External auditing services: https://drata.com/partners/audit-alliance/directory?f_ideal-client-size=smb-1-300-fte&f_industry-specialization=healthcare&f_regions-covered=united-states a. Sensiba LLP b. Insight Assurance c. A-LIGN d. IS Partners, LLC e. Zero Day CPA, PC f. BARR Advisory g. Schellman h. 360 Advanced i. Dansa D'Arata Soucia LLP j. Copeland Buhl k. Sentry Assurance l. Schneider Downs & Co. m. ARORA Solutions LLC n. Audit Peak o. AARC - 360 p. JoHanson Group LLP q. MHM Professional Corporation r. Linford and Company LLP

	s. Boulay t. Please Bell CPAs LLC 7. Startup-friendly offerings a. Built with AI. Replaces spreadsheets, guesswork, and manual tasks with an agentic platform for compliance and trust. b. Automates compliance for SOC 2, ISO 27001, GDPR, HIPAA, etc. c. Automated tests continuously collect evidence, and guided workflows help launch initial frameworks. With multimedia framework support, it's easy to add additional frameworks when you need them d. Give buyers a simple, always on place to access key trust documentation and common answers. You control access to personally branded Trust Centers so prospects can self-serve trust reviews and Wenixco can spend less chasing finding documents over email. 8. Estimated pricing ranges (focus on cost-effective options) a. Data pricing is custom and varies by scope. Offering to put me in touch with a sales team and send pricing requests. 9. Advantages/disadvantages for Wenixo's current stage a. Advantages: i. Less manual work: Automated evidence collection and continuous control monitoring can replace a lot of spreadsheet chasing. ii. Faster path to audit readiness: Guided workflows help first-time teams get organized for SOC 2, ISO 27001, HIPAA, and more. iii. Scales as you grow: You can start with one framework (often SOC 2) and expand without rebuilding everything from scratch. iv. Easier to prove trust: A Trust Center and AI-assisted questionnaire support can reduce time spent on buyer security reviews. b. Disadvantages: i. Cost can add up with breadth: If you want multiple frameworks plus add-on modules (risk, vendor risk, Trust Center), the scope can get expensive for an early-stage budget.

	ii. You still need internal ownership: Automation helps, but someone still needs to define scope, assign control owners, remediate gaps, and manage policies. 10. Whether services are more appropriate for: a. They offer a wide range of products and are ready for any stage of a company

COMPANY #3: SECUREFRAME

Secureframe: https://secureframe.com/pricing Company overview Services offered HIPAA/security/compliance capabilities SOC 2 / HITRUST / ISO certifications supported Audit readiness support External auditing services Startup-friendly offerings Estimated pricing ranges (focus on cost-effective options) Advantages/disadvantages for Wenixo's current stage Whether services are more appropriate for: b. early-stage startups c. scaling startups d. enterprise healthcare systems	1. Company Overview: a. The company is better suited for startups. It was founded in 2020, has over 200 employees, 150 integration, and $79 million in funding.They have 6 hubs across 3 different countries. 2. Services offered a. Secureframe AI: Command line interface, cloud development kit, azure resource manager, google cloud deployment manager, terraform. Auto-generated fixes for infrastructure as code so you can easily copy, paste, and deploy fixes to the cloud environment. i. Comply AI for Remediation: Automated evidence collection, quick view of test status, map controls and tests, test library, assign owners to tests, fast and flexible remediation, export evidence, scope individual resources, custom automated tests. ii. Comply AI for Risk: Produces an inherent risk score, treatment plan, and residual risk score so organizations can improve their risk awareness and response iii. Comply AI for Policies: Edit and revise your policies using the AI-powered text editor to create clear policies that align with the tone and voice of organization. Custom policy templates, comprehensive and

	collaborative editing toolset, AI-powdered text revisions, Assign owners and track versions, Policy addendums, track policy acceptance. iv. Comply AI for Third Party Risk Management (TPRM): Automatically extracting answers from vendor documents like SOC 2 reports for security reviews. Secureframe will then populate suggested answers to the platform for you to review. Centralized third-party risk management, continuously monitor your vendor risk, comply with AI for TPRM, customize third party risk programs. v. Comply AI for Control Mapping: Leverage advanced machine learning and natural language processing to intelligently suggest control mappings to frameworks and risk assessments, reducing manual efforts and freeing up time for teams. Comprehensive view into security posture, save time with common controls, customize your controls, faster remediation with comply AI for remediation. vi. Trust AI for Questionnaire Automation: Leverage machine learning-powdered automation to save hundreds of hours answering RFPs and security questionnaires vii. AI Evidence Validation: Accelerate audit readiness and reduce findings. b. Controls: i. Comprehensive view into security posture: Access a full list of controls that apply to the organization. Monitor control health and see which framework requirements and tests are mapped to each of your controls. ii. Common controls: You can map one control across multiple framework requirements. All frameworks utilize common controls to ensure a sleek

	compliance program. Create custom controls that map to framework requirements, and adjust test mappings. Assess the health status of each control, see mapped framework requirements and tests, assign owners, and find AI-generated remediation guidance for failing controls. c. Automated Evidence Collection: i. Quick view of test status: See compliance program at most granular level. Filter and create custom views for tests by attribute such as status, owner, and framework to quickly understand and review compliance status. ii. Map controls and Tests: Map to frameworks like SOC 2 and ISO 27001. iii. Test Library: Find all secureframe and user created custom tests in the Test Library. Having access to an inventory of all tests that may not be directly mapped to specific frameworks allows you to incorporate additional tests and take advantage of the hundreds of automated tests that are already built. iv. Assign owners to tests v. Remediation powered by AI: automatically generates code fixes or selected step-by-step guidance to implement fixes in your console. vi. Export evidence: download all evidence collected or generated by automated tests and operational tasks in bulk through the Secureframe data room, or individually at each framework and control. View and export raw JSON evidence to aid with detailed remediation for your failed tests. Highlights code that requires attention. vii. Scope individual resources d. Policy Management:

	i. Policy templates: Written and approved by former auditors ii. Custom templates: Create own custom policies with adding attributes iii. Comprehensive and collaborative editing toolset: customize policies and leave comments for better collaboration. Advanced tables, find and replace, seamless copy and paste from external sources, and more iv. AI powered text revisions: summarize content, improve writing, simplify language, change tone and voice, and more v. Assign owners and track versions vi. Policy addendums: reviewed and added to existing policy, no need to start over vii. Track policy acceptance e. User Access Reviews: i. Centralize and complete reviews faster: pull user data through custom and native integrations or via CSV upload. Scope systems, assign reviewers, evaluate access, and close reviews in one streamlined workflow. ii. Reviewers confirm ownership and decide whether access should be maintained, modified, revoked, or marked out of scope at the account level. iii. Designate reviewers per system and use recurring schedules, reminders, and status indicators to keep the process moving. f. Risk Management: i. Automatically assess risks with comply AI ii. Assess and document treatment plans in your environment to meet the criteria for frameworks such as SOC 2, ISO 27001, PCI, and HIPAA. Secureframe's Risk Management system follows the ISO 27005

	methodology so you can effectively assess risks in your environment to make smart decisions for your security compliance program. iii. Easily add risks with the risk library: Secureframe provides a risk library that includes NIST risk scenarios for categories like Fraud, Legal, Finance, and IT. Organizations can easily add these risks to their risk register for tracking. iv. Link risks to controls: Link controls to known risks so that you can coordinate risk management strategies with compliance requirements. Advanced machine learning and natural language processing to suggest control mappings to risk assessments. g. Personnel Management: i. Full visibility into who's keeping the organization compliant. ii. Automate personnel onboarding and offboarding iii. Track tasks and send reminders iv. Monitor vendor access v. Create and manage groups h. Third party risk management: i. Centralized third party risk management: vendor profiles, risk assessments, document attachments, and vendor history logs in the vendor tab in-app ii. Continuously monitor vendor risk iii. Comply AI for TPRM i. Trust Center: i. Publish a trust center for prospects and customers to find info about the measures your organization is taking to ensure a secure position. Data is pulled continuously from secureframe, but admins may choose to hide or display content on their trust center ii. Easily manage requests for documents

	iii. Customize trust center for brand j. Vendor Access: Easily review vendor and employee access. Filter by scope, status and vendor, faster audits. Auditors can quickly verify this requirement directly in secureframe. k. Questionnaire Automation l. Security Awareness Training 3. HIPAA/security/compliance capabilities a. HIPAA i. Training: Security awareness training, pci training, pci secure code training, HIPAA training, ii. End to end compliance, easy third party management, continuous monitoring. iii. Create HIPAA privacy and security policies. Access dozens of policies developed and vetted by our in house compliance experts with HIPAA experience. Easy publish to employees for review and acknowledgement through the secureframe platform iv. Train employees about HIPAA best practices. Guide employees through an automated, self-serve training flow. Get progress reports on which employees have completed HIPAA training. v. Send business Associate Agreements to business associates and customers for electronic signature. Store and manage BAAs to ensure compliance. vi. Evaluate and monitor Hipaa safeguards. Assess and comply with safeguards using 150+ integrations vii. Use continuous monitoring for threats and non-compliance b. Defense for CMMC i. Secureframe defense ii. Defense navigator iii. Managed CUI Enclave iv. Automated cloud provisioning v. Managed federal MDM vi. Managed virtual desktops

	vii. SSP & POA&M Management 4. SOC 2 / HITRUST / ISO certifications supported a. SOC 2 b. ISO 27001:2022 c. PCI DSS d. Cyber Essentials e. NYDFS NYCRR 500 f. FTC Safeguards Rule g. ISO 27017 h. Microsoft SSPA i. NIS2 j. Essential 8 k. CIS l. SOX ITGC m. EU DORA n. C5 o. TISAX p. MVSP q. CMMC 2.0 r. NIST 800-53 - High s. NIST 800-53- Moderate t. NIST 800-53 - Low u. NIST 800-171 v. NIST CSF 2.0 w. FedRAMP x. GovRAMP y. CJIS z. TX-RAMP aa. HIPAA bb. ISO27701 cc. GDPR dd. CCPA ee. CPRA ff. NIST AI RMF gg. ISO 42001 hh. EU AI ACT ii. ISO 9001 5. Audit readiness support a. Automated evidence collection b. Continuous control monitoring c. Policy management templates d. Employee training tracking e. Risk assessments and remediation tracking f. Gap assessments g. Audit dashboards & reporting h. Auditory collaboration tools

	i. Integration based evidence syncing j. Readiness checklists/work/flows 6. External auditing services a. Service: i. SOC 2 Audits ii. HIPAA Assessments iii. ISO 27001 Audits iv. PCI DSS Audits v. NIST Assessments vi. Penetration Testing vii. Vulnerability Assessments viii. Gap Assessments ix. Risk Assessments x. Audit Readiness reviews b. Featured Partners: i. Precinct Security & Assurance ii. Johanson Group LLP iii. Insight Assurance 7. Startup-friendly offerings a. Fundamentals Plan: This is secureframes entry-level compliance package and is specifically designed to help smaller companies get compliant fast. It includes: i. Automated evidence collection ii. Policy management iii. Personnel onboarding/offboarding iv. Risk management v. Security awareness training vi. Trust center tools vii. Continuous monitoring b. HIPAA Compliance Automation: i. Administrative safeguards ii. Access control monitoring iii. Employee training tracking iv. Audit readiness evidence collection v. Vendor and personnel management c. 300+ Integrations: i. Integration with common startup tools like google workplace, GitHub, Aws, Microsoft 365. Programs that we already use which can make implementation easier without building compliance processes manually. 8. Estimated pricing ranges (focus on cost-effective options)

	a. Reach out and schedule a DEMO 5/21/26 b. Anticipated Fundaments plan = $7,500 - $20,000 a year 9. Advantages/disadvantages for Wenixo's current stage a. Advantages: i. Good fit for healthcare compliance readiness: Secureframe Training supports frameworks relevant to healthcare and AI companies including HIPAA, SOC 2, GDPR, PCI DSS, and NIST-related standards. That aligns well with the type of trust and compliance posture Wenixo will likely need as it grows. ii. Reduces vendor sprawl:Instead of using one platform for compliance and another for employee cybersecurity training, Secureframe embeds the training directly into its platform. For a small startup, fewer vendors usually means lower administrative overhead and simpler onboarding. iii. The platform automates reminders, tracks completion, and includes built-in quizzes and onboarding assignments. That is valuable for startups without a dedicated compliance or IT department. iv. Role-based training segmentation could become important later for developers, executives, contractors, or healthcare operations staff. Secureframe already supports assigning different training by employee groups. b. Disadvantages: i. May be more than Wenixo currently needs: Secureframe's broader compliance ecosystem could feel heavy relative to the company's current operational maturity. Some features may go underused early on. ii. To fully benefit from Secureframe, Wenixo would likely need to

	integrate systems, organize personnel groups, maintain evidence, and manage compliance workflows. That can consume valuable startup time. 10. Whether services are more appropriate for: early-stage startups a. The best services for startups include HIPAA readiness, SOC 2 Prep, employee security training, basic risk management, automated evidence collection, and policy templates. Small teams need automation more than large governance systems. It can help us appear enterprise ready without having a lot of clients. Helpful for fundraising and initial customer contracts. There are also good programs for scaling startups and enterprises, but lots of good stuff for what we are looking for.

COMPANY #4: VANTA

Vanta: https://www.vanta.com Company overview Services offered HIPAA/security/compliance capabilities SOC 2 / HITRUST / ISO certifications supported Audit readiness support External auditing services Startup-friendly offerings Estimated pricing ranges (focus on cost-effective options) Advantages/disadvantages for Wenixo's current stage Whether services are more appropriate for: e. early-stage startups	1. Company overview a. This seems like the most realistic company we can possibly work with. They have the same structured website as Clearwater, which is much more worldly, but are promoting discounts for startups and responding to the email quickly. They are looking to add us to their team. 2. Services offered a. Automated Compliance, Continuous GRC (Governance, Risk, and Compliance) b. Personnel and Access management c. Risk Management d. Third Party Risk Management e. Questionnaire Automation f. Trust Center g. Streamlined Audits h. Customer Commitments tracking i. Vanta AI

f. scaling startups g. enterprise healthcare systems	j. Their platform integrates with 400+ tools and also offers a Vanta API for custom integrations and workflows 3. HIPAA/security/compliance capabilities a. Vanta specifically positions itself for healthcare by offering tools to protect sensitive information more easily through automating HIPAA and HITRUST compliance. b. Provides: i. Continuous monitoring of controls ii. Automated evidence iii. Collection for audit readiness iv. Pre-built controls and policy template libraries v. Custom monitoring tests and automation vi. Automated notifications for failed tests. 4. SOC 2 / HITRUST / ISO certifications supported a. SOC 2 b. ISO 27001 c. GDPR d. HIPAA e. HITRUST f. USDP g. NIST AI Risk Management Framework h. ISO 42001 i. CMMC j. CJIS k. NIS2 l. DORA m. CPS 234 n. EU AI Act o. Essential Eight p. Cyber Essentials q. FedRAMP r. Custom frameworks. 5. Audit readiness support a. Vanta provides automated evidence collection for audit readiness, basic

reporting and audit workflows, code change and continuous controls monitoring, and an Auditor API across all plan tiers.
    b. Higher tiers add advanced reporting (six customizable reports), advanced control management, custom monitoring tests, and automated access management
    c. When organizations use Vanta for automated compliance, they reduce audit completion times by 50%, according to A-LIGN, one of Vanta's audit partners.

6. External auditing services
    a. Does not directly perform audits but connects customers to vetted audit partners:
    b. All plan tiers include access to Vanta's auditor network and the ability to bring your own auditor.
    c. AICPA peer-reviewed audit firms.
    d. Named audit partners visible on the startup page include:
        i. A-LIGN
        ii. Schellman
        iii. Frazier & Deeter
        iv. Insight Assurance
        v. Prescient Security.

7. Startup-friendly offerings
    a. Vanta offers a Startups program with a $1,000 discount for new customers. Over 1,000 YC-backed and venture-funded startups trust Vanta, and it is rated #1 in SMB Security Compliance on G2 for 10+ consecutive seasons, with 9 out of 10 startups recommending it to peers.
    b. Automatically handling evidence collection and guiding teams step by step, so founders can stay focused on building.
    c. The Essentials plan is positioned as "the fastest, simplest path to compliance, for companies who want to stay focused on building," covering one compliance framework with an agentic policy generator, the Vanta AI Agent, automated evidence

collection, basic reporting, audit workflows, and a Trust Center.

8. Estimated pricing ranges (focus on cost-effective options)
    a. Meeting on Tuesday

9. Advantages/disadvantages for Wenixo's current stage
    a. Advantages:
        i. 400+ integrations, always-on monitoring, and 20,000+ audits completed, it grows alongside the company without requiring context switching.
        ii. The platform provides continuous cloud monitoring, workforce safeguards, vendor risk reviews, and automated access controls right-sized for early-stage teams.
        iii. Strong healthcare-specific positioning covering both HIPAA and HITRUST automation in one platform.
        iv. Startup-friendly auditor partnerships and support from vCISO service partners help teams without in-house security expertise get audit-ready fast.
    b. Disadvantages:
        i. No pricing available
        ii. The Essentials tier only covers one compliance framework, which may be limiting if Wenixo needs both HIPAA and SOC 2 simultaneously from the start (would require upgrading).
        iii. HITRUST is not explicitly listed as included in entry-level tiers and may require higher-tier plans or add-ons. Not sure if we anticipate using this.
        iv. External audits are handled through partner firms, not Vanta directly, adding a potential coordination layer and separate cost.

	10. Whether services are more appropriate for: This is good for early stage startups and scaling startups. Hopefully we can start our growth here and keep building without having to change platforms.

COMPANY #5: SPRINTO

Sprinto: https://sprinto.com/ Company overview Services offered HIPAA/security/compliance capabilities SOC 2 / HITRUST / ISO certifications supported Audit readiness support External auditing services Startup-friendly offerings Estimated pricing ranges (focus on cost-effective options) Advantages/disadvantages for Wenixo's current stage Whether services are more appropriate for: h. early-stage startups i. scaling startups j. enterprise healthcare systems	1. Company overview a. Sprinto is trusted by 3,000+ companies, ranging from Series A to enterprise. Their core differentiator from traditional GRC tools is the claim that other tools automate tasks while Sprinto owns outcomes, detecting change across an organization's security posture, determining what's at risk, and acting across compliance, vendor risk, AI governance, and more. 2. Services offered a. Sprinto's core product suite includes: i. Audit Management ii. Autonomous TPRM (Third Party Risk Management) iii. Unified Commitments iv. AI Governance v. Risk Management vi. Continuous Monitoring vii. Policy Management viii. Trust Center ix. AI Security Questionnaire automation. b. Additional features include: i. Vulnerability Assessment ii. Zones (access control with intelligent zoning) iii. Change Management iv. Doctor Sprinto MDM (device monitoring) v. Access Control vi. People Ops vii. Security Training viii. Automated Evidence Collection.

	c. Sprinto also offers a browser extension, the Sprinto Compliance Extension, that runs compliance end-to-end including integrations, evidence collection, and security questionnaires, all in one place. 3. HIPAA/security/compliance capabilities a. On security monitoring, Sprinto's Continuous Monitoring product provides always-on monitoring for uninterrupted visibility, and its Risk Management product offers intelligent oversight of infosec risks, continuously recalculating inherent and residual risk from live signals across systems, vendors, and compliance posture. b. For AI-specific risks, Sprinto's AI Governance module detects shadow AI tool adoption across an organization, maintains a live registry, classifies risk by data, and maps an organization's AI footprint to ISO 42001, NIST AI RMF, and the EU AI Act. 4. SOC 2 / HITRUST / ISO certifications supported a. Sprinto supports over 200 frameworks. Those explicitly listed include: i. SOC 2 ii. ISO 27001 iii. PCI-DSS iv. CSA STAR v. NIST-CSF vi. HIPAA vii. GDPR viii. ISO 9001 (2015) ix. ISO 42001 x. TISAX xi. CIS xii. ISO 27017 xiii. FCRA xiv. US FedRAMP xv. RBI_SAR xvi. PIPEDA xvii. CCPA xviii. HITRUST.

	5. Audit readiness support a. Uses four autonomous agents for audit readiness: a Scoping Agent that scans the business and stack to identify exactly which controls apply; an Integration Agent that connects to cloud, HR, and work apps to pull auditor-ready evidence in real time; a Fix-It Agent that scans for gaps, fixes what it can, and routes the rest to the right person with context; and an Audit Agent that runs an internal review before the actual audit, validating evidence, checking controls, and flagging weak spots. b. The Complete Audit Dashboard provides a single hub where the team, tools, and audit agent work together, preparing, collaborating, and staying audit-ready so nothing falls through the cracks. 6. External auditing services a. Like Vanta, Sprinto does not directly perform audits but facilitates access to auditors: b. Sprinto maintains an Audit Partners directory where customers can connect with compliance auditors their clients have worked with. c. Sprinto also offers 1:1 guidance from ISO-certified lead auditors who keep compliance on track and get customers audit-ready at every step. 7. Startup-friendly offerings a. Sprinto has a dedicated "Sprinto for Startups" solution described as "fast, simple compliance that accelerates deals," as well as a free AI Compliance Kit for Startups to kickstart security and compliance with AI automation. b. Sprinto's startup messaging directly addresses founders and engineers, positioning the platform as one that sets itself up, the Scoping Agent does discovery and the Integration Agent connects the stack, with teams moving within a day. c. Sprinto also markets to teams starting with only SOC 2, noting that when an enterprise customer later needs ISO 27001, controls

already map across — framing this as one program, not five.

8. Estimated pricing ranges (focus on cost-effective options)
    a. Email sent, they replied and it was forwarded to the team.

9. Advantages/disadvantages for Wenixo's current stage
    a. Advantages:
        i. Unified Commitments module interprets frameworks, regulations, contracts, and internal policies, structures them into machine-readable controls, maps them to the environment, and keeps them continuously updated, particularly useful for healthcare organizations managing overlapping HIPAA, HITRUST, and SOC 2 requirements simultaneously.
        ii. The platform is designed for teams with zero compliance function, with autonomous scoping, integration, gap-fixing, and audit prep agents reducing the need for dedicated compliance headcount.
        iii. 300+ integrations connect across cloud, identity, HR, and SaaS, with changes detected the moment they happen.
        iv. ISO-certified lead auditor support is included as part of the platform, providing a meaningful layer of expert guidance not just referrals to partners.
    b. Disadvantages
        i. No published pricing whatsoever, even less transparency than Vanta, with no tier structure or introductory offers visible on the website.
        ii. No explicit startup discount program comparable to Vanta's published $1,000 offer.

	iii. Sprinto's customer base of 3,000+ companies is significantly smaller than Vanta's 16,000+, suggesting a less mature ecosystem of integrated auditors and partners. iv. Healthcare-specific positioning exists but is less detailed on the website compared to other industry verticals; the healthcare solution page redirects to a demo form rather than detailed content. 10. Whether services are more appropriate for: a. Similar to Vanta. This is good for early stage startups and scaling startups. Hopefully we can start our growth here and keep building without having to change platforms.