



**SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH  
SYSTEM MEDICAL CENTER GOVERNING BOARD  
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



**ITEM: 15.5  
(ID # 22867)**

**MEETING DATE:**  
Tuesday, August 29, 2023

**FROM :** RUHS-MEDICAL CENTER:

**SUBJECT:** RIVERSIDE UNIVERSITY HEALTH SYSTEM - MEDICAL CENTER: Approve the Professional Service Agreement for Information Security Risk Assessment Services with Securance LLC, without seeking competitive bids for one year, All Districts. [Total Cost \$421,200, up to \$42,120 in additional compensation, 100% -Hospital Enterprise Fund - 40050]

**RECOMMENDED MOTION:** That the Board of Supervisors:

1. Approve the Professional Service Agreement for Information Security Risk Assessment Services with Securance LLC, without seeking competitive bids for a total of \$421,200 for one year through June 30, 2024, and authorize the Chair of the Board to sign the Agreement on behalf of the County; and
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based upon the availability of funding and as approved as to form by County Counsel, to sign amendments that exercise the options of the agreement including modifications to the scope of services that stay within the intent of the Agreement, and sign amendments to the compensation provisions that do not exceed the total sum of ten percent (10%) of the total annual cost of the Agreement.

**ACTION:Policy**

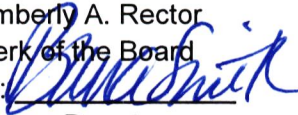
  
Jennifer Cruikshank Chief Executive Officer - Health System 8/21/2023

---

**MINUTES OF THE GOVERNING BOARD**

On motion of Supervisor Spiegel, seconded by Supervisor Perez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

**Ayes:** Jeffries, Spiegel, Washington, Perez and Gutierrez  
**Nays:** None  
**Absent:** None  
**Date:** August 29, 2023  
**xc:** RUHS-Medical Center

Kimberly A. Rector  
 Clerk of the Board  
 By:   
 Deputy

**SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH  
SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS  
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**

<b>FINANCIAL DATA</b>	<b>Current Fiscal Year:</b>	<b>Next Fiscal Year:</b>	<b>Total Cost:</b>	<b>Ongoing Cost</b>
<b>COST</b>	\$ 421,200	\$ 0	\$ 421,200	\$ 0
<b>NET COUNTY COST</b>	\$ 0	\$ 0	\$ 0	\$ 0
<b>SOURCE OF FUNDS:</b> 100% Hospital Enterprise Fund 40050			<b>Budget Adjustment:</b> No	
			<b>For Fiscal Year:</b> 23/24	

**C.E.O. RECOMMENDATION:** Approve

**BACKGROUND:**

**Summary**

Riverside University Health System (RUHS) seeks to enter into a one-year agreement with Securance LLC (“Securance”) for Information Security Risk Assessment Services. The purpose of this service is to identify and evaluate IT technical security risks within the County infrastructure and propose technical solutions to enhance security. Additionally, it aims to help the County achieve compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, which requires periodic risk assessments for all covered entities. The Technical Risk Assessments offered by Securance encompasses various security assessment services, such as Penetration Testing, Vulnerability Assessment, Denial of Service Testing, Social Engineering, Security Architecture and Configuration review, among others. It's emphasized that these assessments can be performed using different tools, techniques, approaches, and methodologies.

**Impact on Residents and Businesses**

These services are a component of RUHS’s system of care aimed at improving the health and safety of its patients and the community.

**Additional Fiscal Information**

There are sufficient funds in the Department’s budget for FY 23/24 budget and no additional County funds are required.

**Contract History and Price Reasonableness**

RUHS seeks to enter into the Professional Service Agreement with Securance to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). Securance was identified as a suitable provider for these services and the price proposed to the County is comparable to pricing offered by other vendors. Securance has also offered the County a “value add price reduction” of \$29,120.

**SUBMITTAL TO THE RIVERSIDE UNIVERSITY HEALTH  
SYSTEM MEDICAL CENTER GOVERNING BOARD OF DIRECTORS  
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**

The proposed Professional Service Agreement requires Board approval per Ordinance 459.6 because it is a purchase of a service costing more than \$50,000 made without securing competitive bids.

ATTACHMENTS:

**Attachment A: Professional Service Agreement for Information Security Risk Assessment Services with Securance LLC**

**Attachment B: SSJ 24-054 Securance LLC**

  
\_\_\_\_\_  
Meghan Hahn, Deputy Director of Procurement 8/21/2023

  
\_\_\_\_\_  
Jacqueline Ruiz, Sr. Management Analyst 8/22/2023

  
\_\_\_\_\_  
Gregg Gu, Chief Deputy County Counsel 8/21/2023

**PROFESSIONAL SERVICE AGREEMENT**

**for**

**Information Security Risk Assessment Services**

**between**

**COUNTY OF RIVERSIDE**

**and**

**Securance LLC**



AUG 29 2023 15.5

**TABLE OF CONTENTS**

<b><u>SECTION HEADING</u></b>	<b><u>PAGE NUMBER</u></b>
1. Description of Services.....	3
2. Period of Performance.....	3
3. Compensation.....	3
4. Alteration or Changes to the Agreement .....	4
5. Termination .....	5
6. Ownership/Use of Contract Materials and Products .....	5
7. Conduct of Contractor .....	6
8. Inspection of Service: Quality Control/Assurance.....	6
9. Independent Contractor/Employment Eligibility .....	7
10. Subcontract for Work or Services.....	8
11. Disputes.....	8
12. Licensing and Permits .....	8
13. Use by Other Political Entities.....	9
14. Non-Discrimination .....	9
15. Records and Documents .....	9
16. Confidentiality .....	9
17. Administration/Contract Liaison .....	10
18. Notices.....	10
19. Force Majeure.....	10
20. EDD Reporting Requirements.....	10
21. Hold Harmless/Indemnification .....	11
22. Insurance .....	11
23. General .....	15
Exhibit A- Payment Provisions.....	18
Exhibit B-Scope of Services .....	23
Attachment I-HIPAA Business Associate Attachment to the Agreement .....	71

This Agreement is made and entered by and between Securance LLC, a Florida limited liability company (herein referred to as "CONTRACTOR"), and the COUNTY OF RIVERSIDE, a political subdivision of the State of California, (herein referred to as "COUNTY"). The parties agree as follows:

**1. Description of Services**

**1.1** CONTRACTOR shall provide all services as outlined and specified in Exhibit B, Scope of Services, at the prices stated in Exhibit A, Payment Provisions, and Attachment I, HIPAA Business Associate Attachment to the Agreement.

**1.2** CONTRACTOR represents that it has the skills, experience, and knowledge necessary to perform under this Agreement and the COUNTY relies upon this representation. CONTRACTOR shall perform to the satisfaction of the COUNTY and in conformance to and consistent with the highest standards of firms/professionals in the same discipline in the State of California.

**1.3** CONTRACTOR affirms this it is fully apprised of all of the work to be performed under this Agreement; and the CONTRACTOR agrees it can properly perform this work at the prices stated in Exhibit A. CONTRACTOR is not to perform services or provide products outside of the Agreement.

**1.4** Acceptance by the COUNTY of the CONTRACTOR's performance under this Agreement does not operate as a release of CONTRACTOR's responsibility for full compliance with the terms of this Agreement.

**2. Period of Performance**

**2.1** This Agreement shall be effective upon signature of this Agreement by both parties and continues in effect through June 30, 2024 unless terminated earlier. CONTRACTOR shall commence performance upon signature of this Agreement by both parties and shall diligently and continuously perform thereafter. The Riverside County Board of Supervisors is the only authority that may obligate the County for a non-cancelable multi-year agreement.

**3. Compensation**

**3.1** The COUNTY shall pay the CONTRACTOR for services performed, products provided and expenses incurred in accordance with the terms of Exhibit A, Payment Provisions. Maximum payments by COUNTY to CONTRACTOR shall not exceed \$421,200 for all expenses. The COUNTY is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or products. Unless otherwise specifically stated in Exhibit A, COUNTY shall not be responsible for payment of any of CONTRACTOR's expenses related to this Agreement.

**3.2** No price increases will be permitted during the first year of this Agreement (If applicable). All price decreases (for example, if CONTRACTOR offers lower prices to another governmental entity) will automatically be extended to the COUNTY. The COUNTY requires written proof satisfactory to COUNTY of cost increases prior to any approved price adjustment. After the first year of the award, a minimum of 30-days advance notice in writing is

required to be considered and approved by COUNTY. No retroactive price adjustments will be considered. Any price increases must be stated in a written amendment to this Agreement. The net dollar amount of profit will remain firm during the period of the Agreement. Annual increases shall not exceed the Consumer Price Index- All Consumers, All Items - Greater Los Angeles, Riverside and Orange County areas and be subject to satisfactory performance review by the COUNTY and approved (if needed) for budget funding by the Board of Supervisors.

**3.3** CONTRACTOR shall be paid only in accordance with an invoice submitted to COUNTY by CONTRACTOR within fifteen (15) days from the last day of each calendar month, and COUNTY shall pay the invoice within thirty (30) working days from the date of receipt of the invoice. Payment shall be made to CONTRACTOR only after services have been rendered or delivery of materials or products, and acceptance has been made by COUNTY. Prepare invoices in duplicate. For this Agreement, send the original and duplicate copies of invoices to:

- a) **AP@RUHealth.org** Each invoice shall contain a minimum of the following information: invoice number and date; remittance address; bill-to and ship-to addresses of ordering department/division; Agreement number 000000000000000000000000355, quantities; item descriptions, unit prices, extensions, sales/use tax if applicable, and an invoice total.
- b) Invoices shall be rendered monthly in arrears.

**3.4** The COUNTY obligation for payment of this Agreement beyond the current fiscal year end is contingent upon and limited by the availability of COUNTY funding from which payment can be made, and invoices shall be rendered "monthly" in arrears. In the State of California, Government agencies are not allowed to pay excess interest and late charges, per Government Codes, Section 926.10. No legal liability on the part of the COUNTY shall arise for payment beyond June 30 of each calendar year unless funds are made available for such payment. In the event that such funds are not forthcoming for any reason, COUNTY shall immediately notify CONTRACTOR in writing; and this Agreement shall be deemed terminated, have no further force, and effect.

**4. Alteration or Changes to the Agreement**

**4.1** The Board of Supervisors and the COUNTY Purchasing Agent and/or his designee is the only authorized COUNTY representatives who may at any time, by written order, alter this Agreement. If any such alteration causes an increase or decrease in the cost of, or the time required for the performance under this Agreement, an equitable adjustment shall be made in the Agreement price or delivery schedule, or both, and the Agreement shall be modified by written amendment accordingly.

**4.2** Any claim by the CONTRACTOR for additional payment related to this Agreement shall be made in writing by the CONTRACTOR within 30 days of when the CONTRACTOR has or should have notice of any actual or claimed change in the work, which results in additional and unanticipated cost to the CONTRACTOR. If the COUNTY Purchasing Agent decides that the facts provide sufficient justification, he

may authorize additional payment to the CONTRACTOR pursuant to the claim. Nothing in this section shall excuse the CONTRACTOR from proceeding with performance of the Agreement even if there has been a change.

**5. Termination**

**5.1.** COUNTY may terminate this Agreement without cause upon 30 days written notice served upon the CONTRACTOR stating the extent and effective date of termination.

**5.2** COUNTY may, upon five (5) days written notice terminate this Agreement for CONTRACTOR's default, if CONTRACTOR refuses or fails to comply with the terms of this Agreement or fails to make progress that may endanger performance and does not immediately cure such failure. In the event of such termination, the COUNTY may proceed with the work in any manner deemed proper by COUNTY.

**5.3** After receipt of the notice of termination, CONTRACTOR shall:

- (a) Stop all work under this Agreement on the date specified in the notice of termination; and
- (b) Transfer to COUNTY and deliver in the manner as directed by COUNTY any materials, reports or other products, which, if the Agreement had been completed or continued, would have been required to be furnished to COUNTY.

**5.4** After termination, COUNTY shall make payment only for CONTRACTOR's performance up to the date of termination in accordance with this Agreement.

**5.5** CONTRACTOR's rights under this Agreement shall terminate (except for fees accrued prior to the date of termination) upon dishonesty or a willful or material breach of this Agreement by CONTRACTOR; or in the event of CONTRACTOR's unwillingness or inability for any reason whatsoever to perform the terms of this Agreement. In such event, CONTRACTOR shall not be entitled to any further compensation under this Agreement.

**5.6** If the Agreement is federally or State funded, CONTRACTOR cannot be debarred from the System for Award Management (SAM). CONTRACTOR must notify the COUNTY immediately of a debarment. Reference: System for Award Management (SAM) at <https://www.sam.gov> for Central Contractor Registry (CCR), Federal Agency Registration (Fedreg), Online Representations and Certifications Application, and Excluded Parties List System (EPLS)). Excluded Parties Listing System (EPLS) (<http://www.epls.gov>) (Executive Order 12549, 7 CFR Part 3017, 45 CFR Part 76, and 44 CFR Part 17). The System for Award Management (SAM) is the Official U.S. Government system that consolidated the capabilities of CCR/FedReg, ORCA, and EPLS.

**5.7** The rights and remedies of COUNTY provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or this Agreement.

**6. Ownership/Use of Contract Materials and Products**



The CONTRACTOR agrees that all materials, reports or products in any form, including electronic, created by CONTRACTOR for which CONTRACTOR has been compensated by COUNTY pursuant to this Agreement shall be the sole property of the COUNTY. The material, reports or products may be used by the COUNTY for any purpose that the COUNTY deems to be appropriate, including, but not limit to, duplication and/or distribution within the COUNTY or to third parties. CONTRACTOR agrees not to release or circulate in whole or part such materials, reports, or products without prior written authorization of the COUNTY.

**7. Conduct of Contractor**

**7.1** The CONTRACTOR covenants that it presently has no interest, including, but not limited to, other projects or contracts, and shall not acquire any such interest, direct or indirect, which would conflict in any manner or degree with CONTRACTOR's performance under this Agreement. The CONTRACTOR further covenants that no person or subcontractor having any such interest shall be employed or retained by CONTRACTOR under this Agreement. The CONTRACTOR agrees to inform the COUNTY of all the CONTRACTOR's interests, if any, which are or may be perceived as incompatible with the COUNTY's interests.

**7.2** The CONTRACTOR shall not, under circumstances which could be interpreted as an attempt to influence the recipient in the conduct of his/her duties, accept any gratuity or special favor from individuals or firms with whom the CONTRACTOR is doing business or proposing to do business, in accomplishing the work under this Agreement.

**7.3** The CONTRACTOR or its employees shall not offer gifts, gratuity, favors, and entertainment directly or indirectly to COUNTY employees.

**8. Inspection of Service; Quality Control/Assurance**

**8.1** All performance (which includes services, workmanship, materials, supplies and equipment furnished or utilized in the performance of this Agreement) shall be subject to inspection and test by the COUNTY or other regulatory agencies at all times. The CONTRACTOR shall provide adequate cooperation to any inspector or other COUNTY representative to permit him/her to determine the CONTRACTOR's conformity with the terms of this Agreement. If any services performed or products provided by CONTRACTOR are not in conformance with the terms of this Agreement, the COUNTY shall have the right to require the CONTRACTOR to perform the services or provide the products in conformance with the terms of the Agreement at no additional cost to the COUNTY. When the services to be performed or the products to be provided are of such nature that the difference cannot be corrected; the COUNTY shall have the right to: (1) require the CONTRACTOR immediately to take all necessary steps to ensure future performance in conformity with the terms of the Agreement; and/or (2) reduce the Agreement price to reflect the reduced value of the services performed or products provided. The COUNTY may also terminate this Agreement for default and

charge to CONTRACTOR any costs incurred by the COUNTY because of the CONTRACTOR's failure to perform.

**8.2** CONTRACTOR shall establish adequate procedures for self-monitoring and quality control and assurance to ensure proper performance under this Agreement; and shall permit a COUNTY representative or other regulatory official to monitor, assess, or evaluate CONTRACTOR's performance under this Agreement at any time, upon reasonable notice to the CONTRACTOR.

**9. Independent Contractor/Employment Eligibility**

**9.1** The CONTRACTOR is, for purposes relating to this Agreement, an independent contractor and shall not be deemed an employee of the COUNTY. It is expressly understood and agreed that the CONTRACTOR (including its employees, agents, and subcontractors) shall in no event be entitled to any benefits to which COUNTY employees are entitled, including but not limited to overtime, any retirement benefits, worker's compensation benefits, and injury leave or other leave benefits. There shall be no employer-employee relationship between the parties; and CONTRACTOR shall hold COUNTY harmless from any and all claims that may be made against COUNTY based upon any contention by a third party that an employer-employee relationship exists by reason of this Agreement. It is further understood and agreed by the parties that CONTRACTOR in the performance of this Agreement is subject to the control or direction of COUNTY merely as to the results to be accomplished and not as to the means and methods for accomplishing the results.

**9.2** CONTRACTOR warrants that it shall make its best effort to fully comply with all federal and state statutes and regulations regarding the employment of aliens and others and to ensure that employees performing work under this Agreement meet the citizenship or alien status requirement set forth in federal statutes and regulations. CONTRACTOR shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by federal or state statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. CONTRACTOR shall retain all such documentation for all covered employees, for the period prescribed by the law.

**9.3** Ineligible Person shall be any individual or entity who: Is currently excluded, suspended, debarred or otherwise ineligible to participate in the federal health care programs; or has been convicted of a criminal offense related to the provision of health care items or services and has not been reinstated in the federal health care programs after a period of exclusion, suspension, debarment, or ineligibility.

**9.4** CONTRACTOR shall screen prospective Covered Individuals prior to hire or engagement. CONTRACTOR shall not hire or engage any Ineligible Person to provide services directly relative to this Agreement. CONTRACTOR shall screen all current Covered Individuals within sixty (60) days of execution of this Agreement to ensure that they have not become Ineligible Persons unless CONTRACTOR has performed such screening on same Covered Individuals under a separate agreement with COUNTY within

the past six (6) months. Covered Individuals shall be required to disclose to CONTRACTOR immediately any debarment, exclusion or other event that makes the Covered Individual an Ineligible Person. CONTRACTOR shall notify COUNTY within five (5) business days after it becomes aware if a Covered Individual providing services directly relative to this Agreement becomes debarred, excluded or otherwise becomes an Ineligible Person.

**9.5** CONTRACTOR acknowledges that Ineligible Persons are precluded from providing federal and state funded health care services by contract with COUNTY in the event that they are currently sanctioned or excluded by a federal or state law enforcement regulatory or licensing agency. If CONTRACTOR becomes aware that a Covered Individual has become an Ineligible Person, CONTRACTOR shall remove such individual from responsibility for, or involvement with, COUNTY business operations related to this Agreement.

**9.6** CONTRACTOR shall notify COUNTY within five (5) business days if a Covered Individual or entity is currently excluded, suspended or debarred, or is identified as such after being sanction screened. Such individual or entity shall be promptly removed from participating in any activity associated with this Agreement.

**10. Subcontract for Work or Services**

No contract shall be made by the CONTRACTOR with any other party for furnishing any of the work or services under this Agreement without the prior written approval of the COUNTY; but this provision shall not require the approval of contracts of employment between the CONTRACTOR and personnel assigned under this Agreement, or for parties named in the proposal and agreed to under this Agreement.

**11. Disputes**

**11.1** The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. Any dispute relating to this Agreement, which is not resolved by the parties, shall be decided by the COUNTY's Purchasing Department's Compliance Contract Officer who shall furnish the decision in writing. The decision of the COUNTY's Compliance Contract Officer shall be final and conclusive unless determined by a court of competent jurisdiction to have been fraudulent, capricious, arbitrary, or so grossly erroneous to imply bad faith. The CONTRACTOR shall proceed diligently with the performance of this Agreement pending the resolution of a dispute.

**11.2** Prior to the filing of any legal action related to this Agreement, the parties shall be obligated to attend a mediation session in Riverside County before a neutral third party mediator. A second mediation session shall be required if the first session is not successful. The parties shall share the cost of the mediations.

**12. Licensing and Permits**

CONTRACTOR shall comply with all State or other licensing requirements, including but not limited to the provisions of Chapter 9 of Division 3 of the Business and Professions Code. All licensing requirements shall be met at the time proposals are submitted to the COUNTY. CONTRACTOR warrants that it has all necessary permits, approvals, certificates, waivers and exemptions necessary for performance of this Agreement as required by the laws and regulations of the United States, the State of California, the County of Riverside and all other governmental agencies with jurisdiction, and shall maintain these throughout the term of this Agreement.

**13. Use By Other Political Entities**

The CONTRACTOR agrees to extend the same pricing, terms, and conditions as stated in this Agreement to each and every political entity, special district, and related non-profit. It is understood that other entities shall make purchases in their own name, make direct payment, and be liable directly to the CONTRACTOR; and COUNTY shall in no way be responsible to CONTRACTOR for other entities' purchases.

**14. Non-Discrimination**

CONTRACTOR shall not be discriminate in the provision of services, allocation of benefits, accommodation in facilities, or employment of personnel on the basis of ethnic group identification, race, religious creed, color, national origin, ancestry, physical handicap, medical condition, marital status or sex in the performance of this Agreement; and, to the extent they shall be found to be applicable hereto, shall comply with the provisions of the California Fair Employment and Housing Act (Gov. Code 12900 et. seq), the Federal Civil Rights Act of 1964 (P.L. 88-352), the Americans with Disabilities Act of 1990 (42 U.S.C. S1210 et seq.) and all other applicable laws or regulations.

**15. Records and Documents**

CONTRACTOR shall make available, upon written request by any duly authorized Federal, State, or COUNTY agency, a copy of this Agreement and such books, documents and records as are necessary to certify the nature and extent of the CONTRACTOR's costs related to this Agreement. All such books, documents and records shall be maintained by CONTRACTOR for at least five years following termination of this Agreement and be available for audit by the COUNTY. CONTRACTOR shall provide to the COUNTY reports and information related to this Agreement as requested by COUNTY.

**16. Confidentiality**

**16.1** The CONTRACTOR shall not use for personal gain or make other improper use of privileged or confidential information which is acquired in connection with this Agreement. The term "privileged or confidential information" includes but is not limited to: unpublished or sensitive technological or scientific information; medical, personnel, or security records; anticipated material requirements or pricing/purchasing actions; COUNTY information or data which is not subject to public disclosure; COUNTY operational

procedures; and knowledge of selection of contractors, subcontractors or suppliers in advance of official announcement.

**16.2** The CONTRACTOR shall protect from unauthorized disclosure names and other identifying information concerning persons receiving services pursuant to this Agreement, except for general statistical information not identifying any person. The CONTRACTOR shall not use such information for any purpose other than carrying out the CONTRACTOR's obligations under this Agreement. The CONTRACTOR shall promptly transmit to the COUNTY all third party requests for disclosure of such information. The CONTRACTOR shall not disclose, except as otherwise specifically permitted by this Agreement or authorized in advance in writing by the COUNTY, any such information to anyone other than the COUNTY. For purposes of this paragraph, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particulars assigned to the individual, such as finger or voice print or a photograph.

**16.3** The CONTRACTOR is subject to and shall operate in compliance with all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, and the related laws and regulations promulgated subsequent thereto. Please refer to Attachment 1 of this agreement.

**17. Administration/Contract Liaison**

The COUNTY Purchasing Agent, or designee, shall administer this Agreement on behalf of the COUNTY. The Purchasing Department is to serve as the liaison with CONTRACTOR in connection with this Agreement.

**18. Notices**

All correspondence and notices required or contemplated by this Agreement shall be delivered to the respective parties at the addresses set forth below and are deemed submitted two days after their deposit in the United States mail, postage prepaid:

**COUNTY OF RIVERSIDE**

Riverside University Health System – Medical  
Center - Information Services  
26520 Cactus Ave, Moreno Valley, CA 92555

**CONTRACTOR**

**Securance LLC**  
13916 Monroes Business Park, Suite  
102  
Tampa, FL 33635

**19. Force Majeure**

If either party is unable to comply with any provision of this Agreement due to causes beyond its reasonable control, and which could not have been reasonably anticipated, such as acts of God, acts of war, civil disorders, or other similar acts, such party shall not be held liable for such failure to comply.

**20. EDD Reporting Requirements**

In order to comply with child support enforcement requirements of the State of California, the COUNTY may be required to submit a Report of Independent Contractor(s) form **DE 542** to the Employment Development Department. The CONTRACTOR agrees to furnish the required data and certifications to the COUNTY within 10 days of notification of award of Agreement when required by the EDD. This data will be transmitted to governmental agencies charged with the establishment and enforcement of child support orders. Failure of the CONTRACTOR to timely submit the data and/or certificates required may result in the contract being awarded to another contractor. In the event a contract has been issued, failure of the CONTRACTOR to comply with all federal and state reporting requirements for child support enforcement or to comply with all lawfully served Wage and Earnings Assignments Orders and Notices of Assignment shall constitute a material breach of Agreement. If CONTRACTOR has any questions concerning this reporting requirement, please call (916) 657-0529. CONTRACTOR should also contact its local Employment Tax Customer Service Office listed in the telephone directory in the State Government section under "Employment Development Department" or access their Internet site at [www.edd.ca.gov](http://www.edd.ca.gov).

**21. Hold Harmless/Indemnification**

**21.1** CONTRACTOR shall indemnify and hold harmless the County of Riverside, its Agencies, Districts, Special Districts and Departments, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability, action, claim or damage whatsoever, based or asserted upon any services of CONTRACTOR, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Agreement, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature. CONTRACTOR shall defend the Indemnitees at its sole expense including all costs and fees (including, but not limited, to attorney fees, cost of investigation, defense and settlements or awards) in any claim or action based upon such acts, omissions or services.

**21.2** With respect to any action or claim subject to indemnification herein by CONTRACTOR, CONTRACTOR shall, at their sole cost, have the right to use counsel of their own choice and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of COUNTY; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes CONTRACTOR indemnification to Indemnitees as set forth herein.

**21.3** CONTRACTOR'S obligation hereunder shall be satisfied when CONTRACTOR has provided to COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim involved.

**21.4** The specified insurance limits required in this Agreement shall in no way limit or circumscribe CONTRACTOR'S obligations to indemnify and hold harmless the Indemnitees herein from third party claims.

**22. Insurance**

**22.1** Without limiting or diminishing the CONTRACTOR'S obligation to indemnify or hold the COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents, or representatives as Additional Insureds.

**A. Workers' Compensation:**

If the CONTRACTOR has employees as defined by the State of California, the CONTRACTOR shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than \$1,000,000 per person per accident. The policy shall be endorsed to waive subrogation in favor of The County of Riverside.

**B. Commercial General Liability:**

Commercial General Liability insurance coverage, including but not limited to, premises liability, unmodified contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of CONTRACTOR'S performance of its obligations hereunder. Policy shall name the COUNTY as Additional Insured. Policy's limit of liability shall not be less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit.

**C. Vehicle Liability:**

If vehicles or mobile equipment is used in the performance of the obligations under this Agreement, then CONTRACTOR shall maintain liability insurance for all owned, non-owned, or hired vehicles so used in an amount not less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit. Policy shall name the COUNTY as Additional Insureds.

**D. Professional Liability** Contractor shall maintain Professional Liability Insurance providing coverage for the Contractor's performance of work included within this Agreement, with a limit of liability of not less than \$1,000,000 per occurrence and \$2,000,000 annual aggregate. If Contractor's Professional Liability Insurance is written on a claims made basis rather than an occurrence basis, such insurance shall continue through the term of this Agreement and CONTRACTOR shall purchase at his sole expense either 1) an Extended Reporting Endorsement (also, known as Tail Coverage); or 2) Prior Dates Coverage from new insurer with a retroactive date back to the date of, or prior to, the inception of this Agreement; or 3) demonstrate through Certificates of Insurance that CONTRACTOR has Maintained continuous coverage with the same or original insurer. Coverage provided under items; 1), 2), or 3) will continue as long as the law allows.

**E. Cyber Liability:** CONTRACTOR shall procure and maintain cyber liability insurance, with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CONTRACTOR in this Agreement and shall include, but not limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

If CONTRACTOR maintains broader coverage and/or higher limits than the minimums shown above, COUNTY requires and shall be entitled to the broader coverage and/or higher limits maintained by CONTRACTOR. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to COUNTY

**F. General Insurance Provisions - All lines:**

1) Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an A M BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.

2) The CONTRACTOR must declare its insurance self-insured retention for each coverage required herein. If any such self-insured retention exceeds \$500,000 per occurrence each such retention shall have the prior written consent of the County Risk Manager before the commencement of operations under this Agreement. Upon notification of self-insured retention unacceptable to the COUNTY, and at the election of the County's Risk Manager, CONTRACTOR'S carriers shall either; 1) reduce or eliminate such self-insured retention as respects this Agreement with the COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.

3) CONTRACTOR shall cause CONTRACTOR'S insurance carrier(s) to furnish the County of Riverside with either 1) a properly executed original Certificate(s) of Insurance and certified original copies of Endorsements effecting coverage as required herein, and 2) if requested to do so orally or in writing by the County Risk Manager, provide original Certified copies of policies including all Endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance carrier(s) that thirty (30) days written notice shall be given to the County of Riverside prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event of a material modification, cancellation, expiration, or reduction in



coverage, this Agreement shall terminate forthwith, unless the County of Riverside receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverage's set forth herein and the insurance required herein is in full force and effect. CONTRACTOR shall not commence operations until the COUNTY has been furnished original Certificate (s) of Insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this Section. An individual authorized by the insurance carrier shall sign the original endorsements for each policy and the Certificate of Insurance.

4) It is understood and agreed to by the parties hereto that the CONTRACTOR'S insurance shall be construed as primary insurance, and the COUNTY'S insurance and/or deductibles and/or self-insured retention's or self-insured programs shall not be construed as contributory.

5) If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services; or, there is a material change in the equipment to be used in the performance of the scope of work; or, the term of this Agreement, including any extensions thereof, exceeds five (5) years; the COUNTY reserves the right to adjust the types of insurance and the monetary limits of liability required under this Agreement, if in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by the CONTRACTOR has become inadequate.

6) CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.

7) The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to the COUNTY.

8) CONTRACTOR agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.

### **23. General**

**23.1** CONTRACTOR shall not delegate or assign any interest in this Agreement, whether by operation of law or otherwise, without the prior written consent of COUNTY. Any attempt to delegate or assign any interest herein shall be deemed void and of no force or effect.

**23.2** Any waiver by COUNTY of any breach of any one or more of the terms of this Agreement shall not be construed to be a waiver of any subsequent or other breach of the same or of any other term of this Agreement. Failure on the part of COUNTY to require exact, full, and complete compliance with any terms of this Agreement shall not be construed as in any manner changing the terms or preventing COUNTY from enforcement of the terms of this Agreement.

**23.3** In the event the CONTRACTOR receives payment under this Agreement, which is later disallowed by COUNTY for nonconformance with the terms of the Agreement, the CONTRACTOR shall

promptly refund the disallowed amount to the COUNTY on request; or at its option the COUNTY may offset the amount disallowed from any payment due to the CONTRACTOR.

**23.4** CONTRACTOR shall not provide partial delivery or shipment of services or products unless specifically stated in the Agreement.

**23.5** CONTRACTOR shall not provide any services or products subject to any chattel mortgage or under a conditional sales contract or other agreement by which an interest is retained by a third party. The CONTRACTOR warrants that it has good title to all materials or products used by CONTRACTOR or provided to COUNTY pursuant to this Agreement, free from all liens, claims, or encumbrances.

**23.6** Nothing in this Agreement shall prohibit the COUNTY from acquiring the same type or equivalent equipment, products, materials or services from other sources, when deemed by the COUNTY to be in its best interest. The COUNTY reserves the right to purchase more or less than the quantities specified in this Agreement.

**23.7** The COUNTY agrees to cooperate with the CONTRACTOR in the CONTRACTOR's performance under this Agreement, including, if stated in the Agreement, providing the CONTRACTOR with reasonable facilities and timely access to COUNTY data, information, and personnel.

**23.8** CONTRACTOR shall comply with all applicable Federal, State and local laws and regulations. CONTRACTOR will comply with all applicable COUNTY policies and procedures. In the event that there is a conflict between the various laws or regulations that may apply, the CONTRACTOR shall comply with the more restrictive law or regulation.

**23.9** CONTRACTOR shall comply with all air pollution control, water pollution, safety and health ordinances, statutes, or regulations, which apply to performance under this Agreement.

**23.10** CONTRACTOR shall comply with all requirements of the Occupational Safety and Health Administration (OSHA) standards and codes as set forth by the U.S. Department of Labor and the State of California (Cal/OSHA).

**23.11** This Agreement shall be governed by the laws of the State of California. Any legal action related to the performance or interpretation of this Agreement shall be filed only in the Superior Court of the State of California located in Riverside, California, and the parties waive any provision of law providing for a change of venue to another location. In the event any provision in this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force without being impaired or invalidated in any way.

**23.12** This Agreement, including any attachments or exhibits, constitutes the entire Agreement of the parties with respect to its subject matter and supersedes all prior and contemporaneous representations, proposals, discussions and communications, whether oral or in writing. This Agreement may be changed or modified only by a written amendment signed by authorized representatives of both parties.

**23.13** This Agreement may be executed in any number of counterparts, each of which will be an original, but all of which together will constitute one instrument. Each party of this Agreement agrees to the use of electronic signatures, such as digital signatures that meet the requirements of the California Uniform Electronic Transactions Act (“CUETA”) Cal. Civ. Code §§ 1633.1 to 1633.17), for executing this Agreement. The parties further agree that the electronic signatures of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record pursuant to the CUETA as amended from time to time. The CUETA authorizes use of an electronic signature for transactions and contracts among parties in California, including a government agency. Digital signature means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature, and shall be reasonably relied upon by the parties. For purposes of this section, a digital signature is a type of "electronic signature" as defined in subdivision (h) of Section 1633.2 of the Civil Code.

[Signature Page Follows]

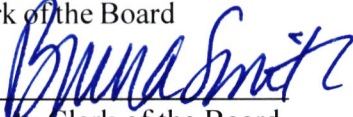
IN WITNESS WHEREOF, the Parties hereto have caused their duly authorized representatives to execute this Agreement.

**COUNTY OF RIVERSIDE**, a political subdivision of the State of California

By:   
Kevin Jeffries, Chairperson  
Board of Supervisors

Dated: 8/29/23

ATTEST:  
Kimberly Rector  
Clerk of the Board

By:   
Deputy Clerk of the Board

APPROVED AS TO FORM:  
Minh C. Tran  
County Counsel

By: Tawny Lieu  
Tawny Lieu (Aug 18, 2023 16:36 PDT)  
Tawny Lieu  
Deputy County Counsel

**Securance LLC**, a Florida limited liability company

By: Paul Ashe  
Name: Paul Ashe  
Title: President

Dated: 08/18/23



# Exhibit A COST PROPOSAL

Securance has provided itemized pricing for the major aspects of this project in the table below.

Project Scope Item	Line Item Fee
<b>Project Management Status Report</b>	\$5,200
<b>Project Management - Engagement Manager</b>	\$15,600
<b>Network Security Assessment</b>	
Firewalls (up to 6)	\$15,600
Routers (up to 20)	\$20,800
Switches (up to 40)	\$41,600
Remote Access - VPN	\$4,160
Intrusion Prevention/Detection System Assessment	\$5,720
Network Architecture Review	\$4,160
External Network Vulnerability Assessment and Penetration Test	\$5,200
Internal Network Vulnerability Assessment and Penetration Test	\$15,600
<b>Host/Server Security</b>	
Virtual Host Server Security Configuration Assessment — VMWare	\$7,800
Server Configuration Assessment (up to 2 brands)	\$6,240
<b>Endpoint Security Review</b>	
Endpoint Security Review (up to 5 brands)	\$7,800
Mobile Device Security Assessment	\$6,500
User Security Awareness Training Review	\$4,160
Social Engineering — Email Phishing   Tailgating (4 locations)	\$5,200
<b>Application Security Assessment</b>	
Enterprise Application Security Testing (7 applications)	\$27,300
Web Application Security Testing (10 applications)	\$13,000
Cloud-Based Services Assessment (3 cloud applications)	\$6,500

## Exhibit A Cost Proposal

Project Scope Item	Line Item Fee
<b>Non-Technical Risk Assessment</b>	
IT Policy, Procedure, Standard, and Guideline Review	\$10,400
User Access and Provisioning Review — Network Layer	\$11,700
NIST CSF Assessment	\$26,000
HIPAA Security, Privacy, Breach Notification Review*	\$62,400
HIPAA Mapping to NIST CSF	\$31,200
HITECH Assessment	\$36,400
On-Site Physical Security Inspection of 6 Specified County Facilities	\$9,360
<b>Executive Summary Report of Findings, Recommendations for Mitigations and Best Practices</b>	\$10,400
<b>Remediation Roadmap</b>	\$5,200
Remote Review of the Findings with County Information Security Office — <b>VALUE ADD</b>	<b>\$3,120</b>
Cybersecurity Posture/Risk Appetite Mapping — <b>VALUE ADD</b>	<b>\$10,400</b>
Knowledge Transfer — <b>VALUE ADD</b>	<b>\$15,600</b>
	<b>Subtotal \$450,320</b>
	<b>Value Add Price Reduction (\$29,120)</b>
	<b>Total \$421,200</b>


\* Listed fee includes a 25% sample of locations, and interviews with all 65 departments. Securance can adjust the fee as locations and departments are reduced. Please request a Best And Final Offer (BAFO) if you would like to reduce locations and departments in scope.

## Exhibit A Cost Proposal

Securance's proposed fees are based on the information that has been made available to us and on our understanding of the engagement, including the assumptions listed above. If the basis of our pricing is inaccurate, then the total cost to complete this engagement may differ from the firm, fixed price in this proposal. If events or circumstances, such as changes in scope, loss or unavailability of County personnel, or unavailability of documentation occur, Securance will determine their effect on the engagement scope, timing, and | or fees and promptly notify County of any such changes. Securance will not proceed with any changes or additions to the scope of work without County's explicit written approval.

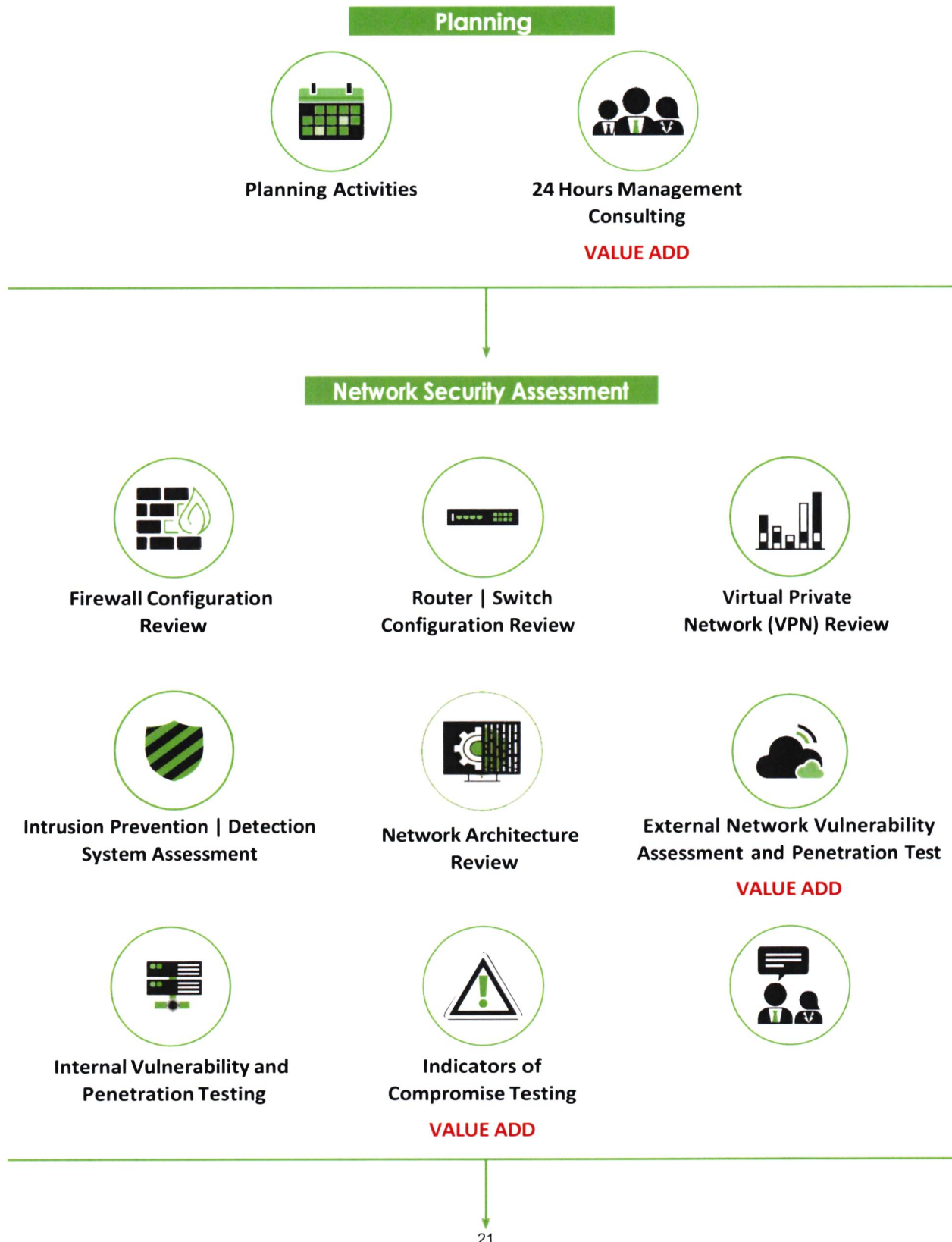
### Hourly Rate

Securance's cost proposal is based on an hourly rate of \$130, inclusive of labor, travel, system licenses, and other reimbursable expenses. The hourly rate applies to all tasks and personnel resources required to complete this project. Any follow-up assessments or consulting engagements will be billed at the same hourly rate..

I, Paul Ashe **CERTIFICATIONS** a duly authorized agent of Securance Consulting  
**Printed Name of Agent/Officer** **Name of Organization**  
hereby certify that Securance Consulting by submission of this proposal in response to the  
**Name of Organization**  
**Professional Services RFP, agree upon contract award to carry out the requirements specified and obligations set forth therein.**  
**Signature**  **Date** 08.15.2027  
**Title of Agent/Officer** President

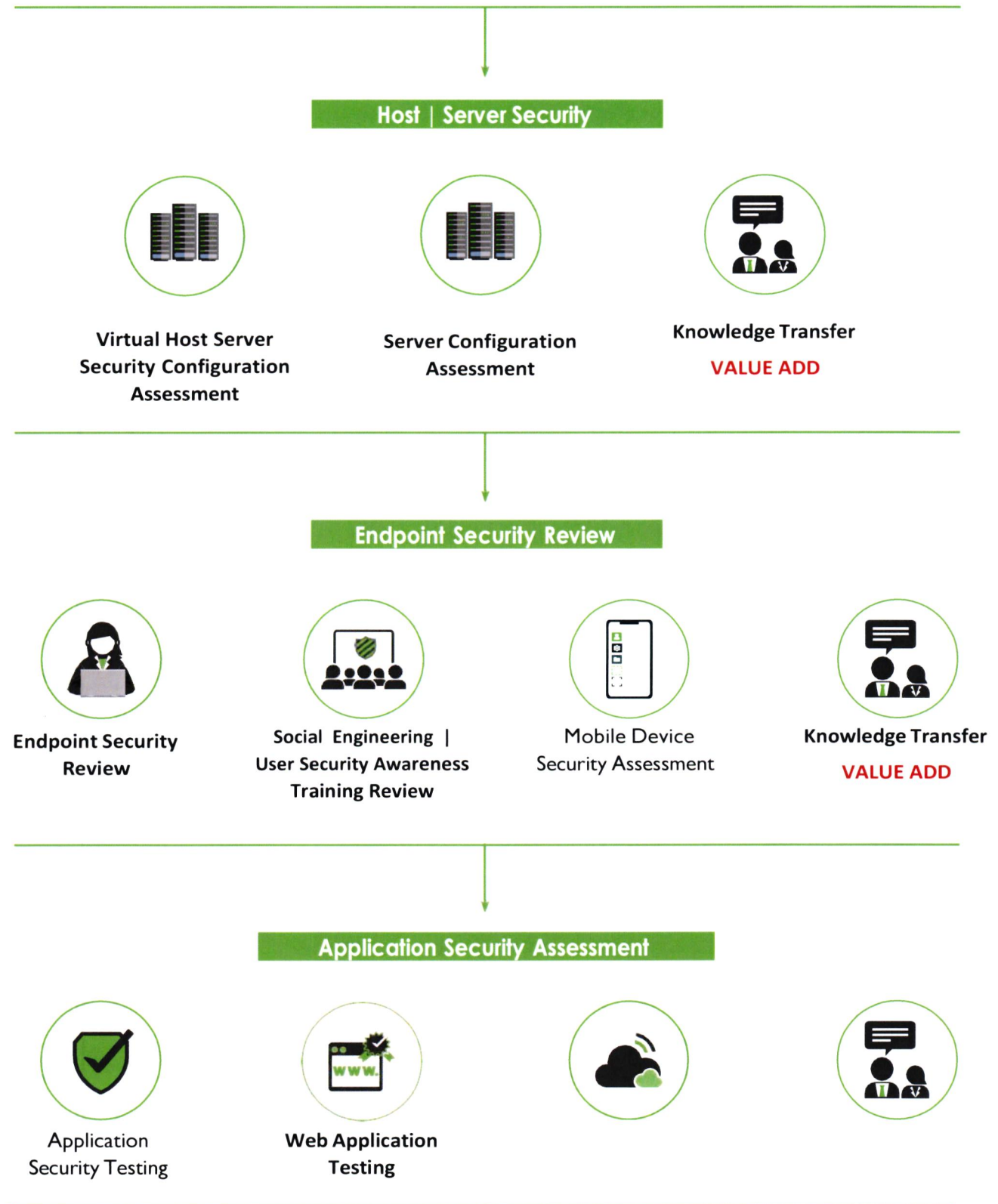
# EXHIBIT B — SCOPE OF SERVICES

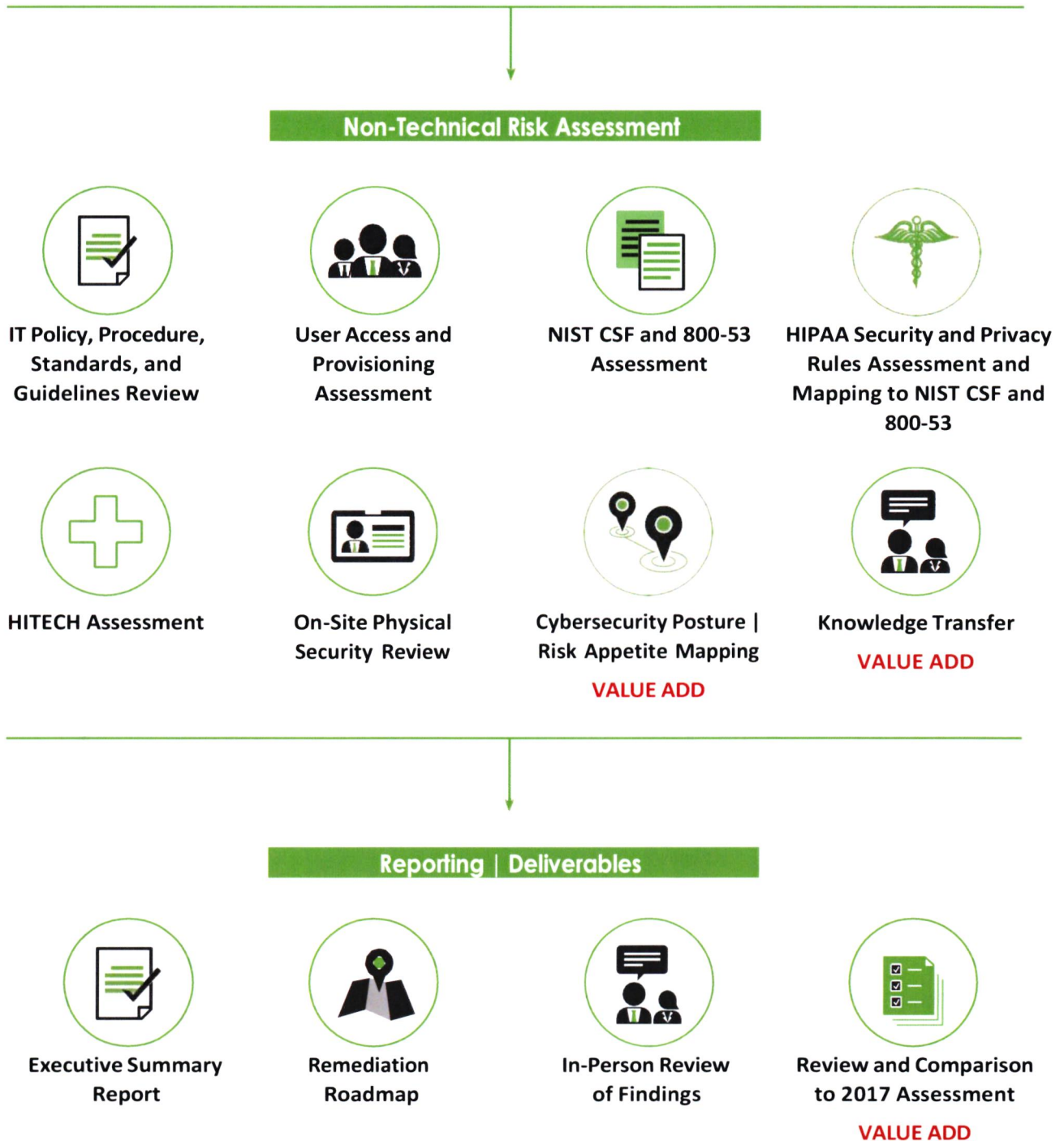
Below we summarize our current understanding of County's project objectives and deliverable expectations.





## — Scope of Services





## — Scope of Services

### 1. Vendor Requirements

1.1 Bidder shall be regularly and continuously engaged in the business of providing the produce and services detailed in this RFP for at least 5 years

Founded on March 4, 2002, Securance has performed more than 1,000 assessments for clients in nearly every industry, and have been providing these services for healthcare and municipal clients for nearly as long. We answer the growing cybersecurity, risk management, and regulatory compliance concerns of governments, school districts, utilities, private companies, universities, banks, transportation authorities, and more.

1.2 Bidder will have previous healthcare Technical Network and Security Risk assessment engagements and are required-a minimum of 5 such references

Securance has conducted numerous technical network and security risk assessments for clients, including healthcare clients, for 20 years. In 2017, we completed a HIPAA Security Assessment for County, in which we provided a comprehensive analysis of compliance with the Privacy and Security Rules and Breach Notification. A list of our references can be found on pages 66-67.

1.3 Bidder must have a Chief Information Officer (CISO) on-staff.

Paul Ashe, Securance President and founder, is the firm's Chief Information Security Officer (CISO).

1.4 Describe the deliverables or tools that will be provided during and after assessment is complete. (i.e., Detailed Reports, Scorecard, Tracking Solution).

County will receive two final reports at the end of the engagement, a management report and a technician's report. The Securance engagement manager will review the reports with County's team and other stakeholders to ensure that County understands the findings and recommendations, and to answer any questions that County may have. In addition, we will provide free technical support and advice throughout the remediation phase.

### Management Report

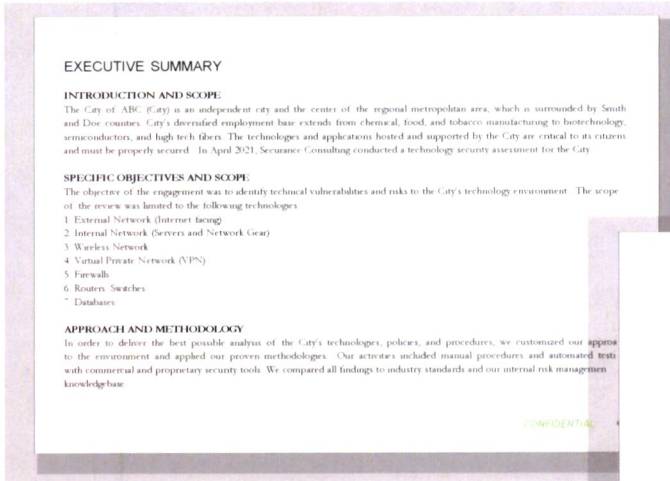
Within one week of completing our fieldwork for the information security risk assessment, Securance will provide County with a board-ready management report tailored to County's environment and needs and developed with input from County's stakeholders and IT management. Our analysis of the risks identified within your environment will take into account County's threat profile, the likelihood and impact of exploitation of existing vulnerabilities, and the controls and security measures already in place. In the management report, we will document our analysis, prioritize risks based on their potential impact on the business, and provide realistic remediation recommendations aligned with County's risk appetite. The report, comprised of three sections, will include an executive summary, a detailed project report, and a remediation roadmap, each of which is described below.

# — Scope of Services

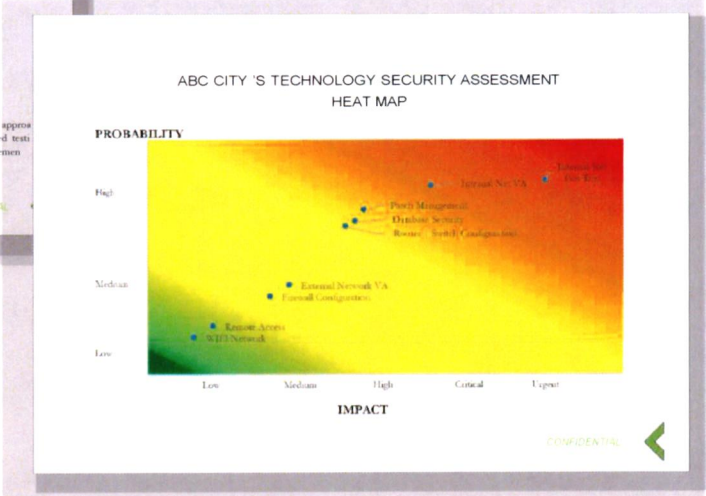
## 1. Vendor Requirements (continued)

### Executive Summary

The executive summary will outline the engagement’s scope, approach, findings, remediation recommendations, and best practices in a manner suitable for management and will be presented to County’s stakeholders during the exit conference. It will include a heat map highlighting identified risks based on their likelihood and impact via a color-coded graph.

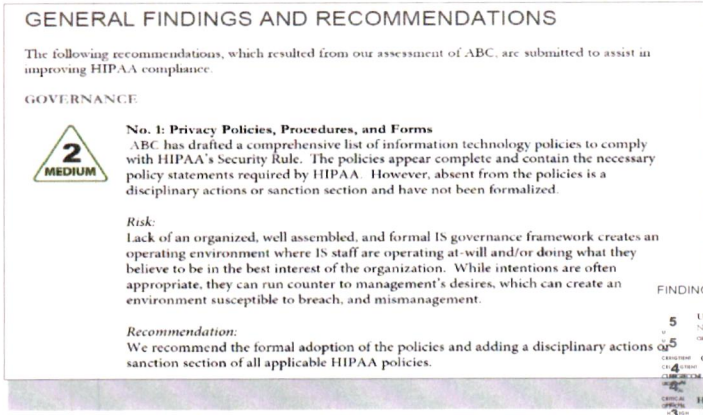


Click on the thumbnails to view the reports.



### Detailed Project Report

The detailed project report will provide specifics regarding the project scope, approach, and methodology, as well as findings and actionable recommendations co-developed by Securance and County.



**FINDING LEGEND**

5	<b>Urgent-Risk (Level 5)</b> - Immediate remediation required. Note: If finding is a technical vulnerability, it provides remote intruders with remote root or administrative capabilities.
4	<b>Critical-Risk (Level 4)</b> - Immediate action recommended, with remediation ASAP. Note: If finding is a technical vulnerability, it provides intruders with remote user, but not remote administrative or root user capabilities.
3	<b>High-Risk (Level 3)</b> - Immediate action recommended, with remediation in 90 days. Note: If finding is a technical vulnerability, it provides intruders with access to sensitive information, including security settings, stored on the host. This level of vulnerabilities could result in potential misuse of the host by intruder.
2	<b>Medium-Risk (Level 2)</b> - Action recommended, with remediation in 180 days. Note: If finding is a technical vulnerability, it may expose sensitive information, such as precise versions of services, from the host. With this information, hackers could research potential attacks to try against a host.
1	<b>Low-Risk/Informational (Level 1)</b> - Effective control. No immediate changes recommended. Opportunity for slight improvement.
A	<b>Advisory Comment</b> - Action suggested at the discretion of management.

Note: Remediation timeframes are based on best practices and Securance's experience.

CONFIDENTIAL

## — Scope of Services

### 1. Vendor Requirements (continued)

#### Remediation Roadmap

The remediation roadmap will list the estimated efforts and costs to remediate urgent, critical, high, and medium risks and vulnerabilities discovered during the assessment.

ROADMAP TO HIPAA COMPLIANCE					
NO.	FINDING TITLE	RISK PRIORITY	ESTIMATED REMEDIATION COST	ESTIMATED REMEDIATION TIMELINE	ESTIMATED RESOURCES
No. 7	Data Loss Prevention	4	\$116,160.00	120 Days	2
No. 8	Active Directory Account Policy Analysis (HIPAA PSA)	4	\$26,400.00	30 Days	2
No. 17	Logging and Monitoring	4	\$316,800.00	180 Days	4
No. 4	Network Design	3	\$59,400.00	45 Days	3
No. 9	Database Security (enabling encryption on HIPAA technologies only)	3	\$19,360.00	30 Days	1
No. 16	Disaster Recovery Plan	3	\$232,320.00	180 Days	2
No. 19	Physical Security and	3	\$75,560.00	180 Days	2

*Click on the thumbnail to view the report.*

#### Technician’s Report

Intended to guide engineers and administrators through the remediation process, the technician’s report will contain raw data extracted from our security tools. While the management report will focus on urgent, critical, high, and medium risks and vulnerabilities that require management’s attention, the technician’s report will cover all vulnerabilities, even low-risk vulnerabilities and advisory comments.

## — Scope of Services

### 1. Vendor Requirements (continued)

I.5 Bidder will have the ability to perform a risk assessment in accordance with NIST Special Publications, NIST Cybersecurity Framework, Health Information Technology for Economic and Clinical Health (HITECH) Act and based on the standards and implementation specifications identified in the HIPAA Security Rule.

Securance will conduct the following assessments in accordance with section I.5 above. Please find details of our HIPAA Security and Privacy Rule Assessment and HITECH Assessment methodologies on pages [23-28](#).



**HIPAA Security  
and Privacy Rules  
Assessment and  
Mapping to NIST CSF**



**HITECH Assessment**

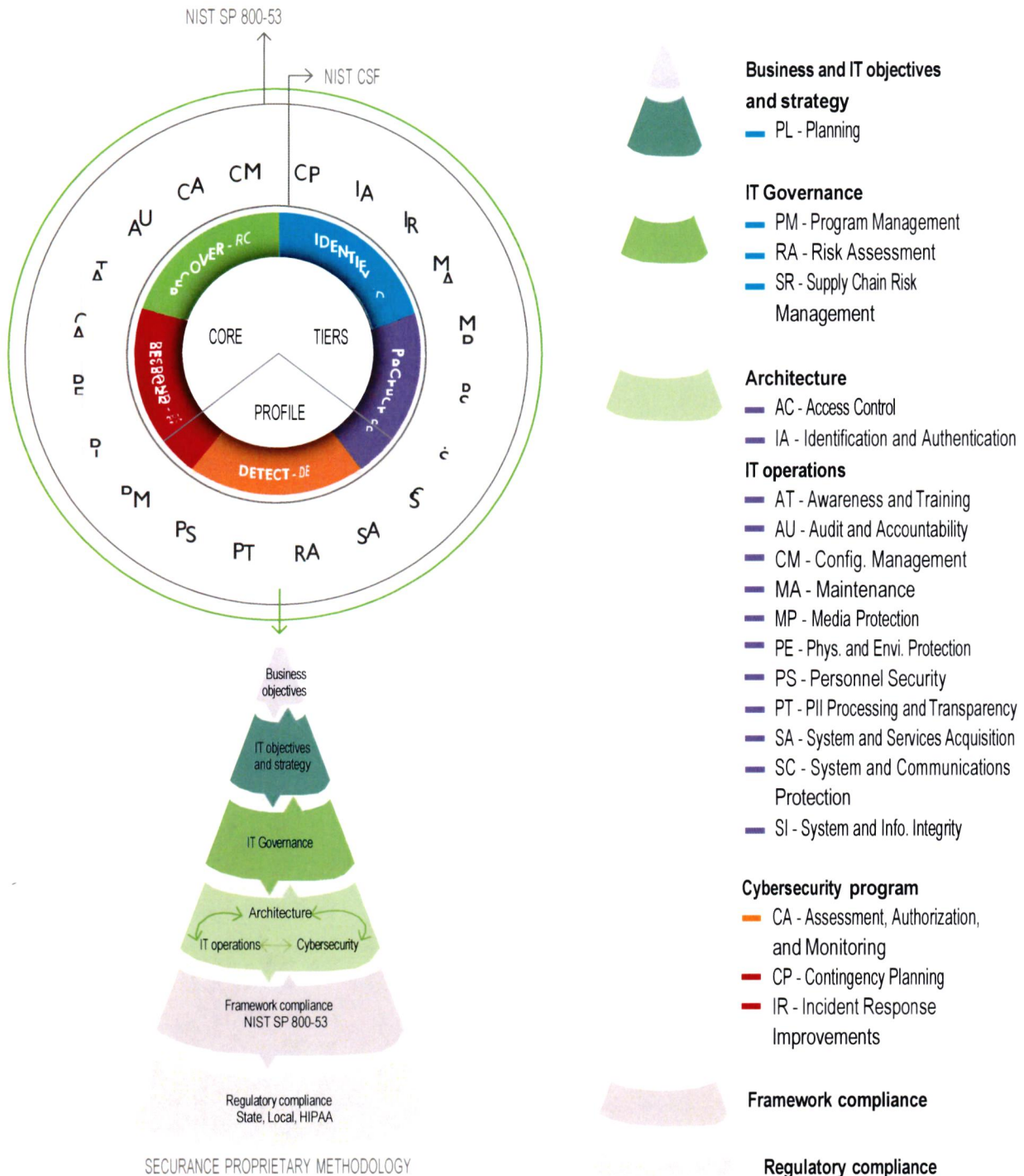
*Remainder of page left intentionally blank*

## — Scope of Services

### 1. Vendor Requirements (continued)

#### HIPAA Security and Privacy Rule Assessment and Mapping to NIST CSF and 800-53

IT general controls (ITGC) are the foundation of the IT organization and ensure the integrity of data and processes supporting IT systems, including applications, databases, and infrastructure. Our assessment approach begins with understanding the organization’s business objectives and strategies and aligns with NIST CSF and SP 800-53.



## — Scope of Services

### 1. Vendor Requirements (continued)

#### HIPAA Security and Privacy Rule Assessment and Mapping to NIST CSF and 800-53 (continued)

##### Our Process

Assess key people, processes, and technologies against the NIST CSF and SP 800-53 to identify control gaps



Review IT governance documents, including IT charters, policies, procedures, standards, and guidelines



Conduct interviews with relevant IT staff to confirm IT controls and technologies that align with NIST CSF and SP 800-53



Perform a gap analysis of the current tier level of security and controls against NIST CSF

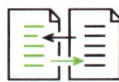


Develop a current state framework profile for County based on NIST CSF tiers of:

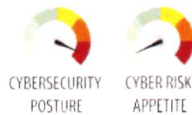
- ◆ Tier 1: Partial
- ◆ Tier 2: Risk-informed
- ◆ Tier 3: Repeatable
- ◆ Tier 4: Adaptive



Map County's NIST CSF Profile and NIST SP 800-53 controls to state, local, and HIPAA, requirements\*



Map results of assessment to cybersecurity posture and cyber risk appetite



Develop a NIST roadmap documenting how to improve tier levels for each NIST control



Develop a compliance and risk mitigation strategy based on the results of the assessment





## — Scope of Services

### 1. Vendor Requirements (continued)

#### HIPAA Security and Privacy Rule Assessment and Mapping to NIST CSF and 800-53 (continued)

#### Sample Mapping Matrix

Below is an illustration of how Securance will map County’s NIST CSF Profile and NIST SP 800-53 controls to state, local, and HIPAA requirements.

#### NIST CSF 800-53

NIST CSF	NIST SP 800-53	HIPAA	CJIS	PCI DSS	SOC 2
<b>ID.AM-1</b>	CM-8 PM-5	Security Rule	Policy Area 7 Policy Area 10	Requirement 2 Requirement 9 Requirement 11 Requirement 12	CC3.2
<b>ID.AM-2</b>	CM-8 PM-5	Security Rule	Policy Area 7 Policy Area 10	Requirement 2 Requirement 12	CC3.2
<b>ID.AM-3</b>	AC-4 CA-3 CA-9 PL-8	Security Rule	Policy Area 10	Requirement 1	CC3.2

## — Scope of Services

### 1. Vendor Requirements (continued)

#### HIPAA Security and Privacy Rule Assessment and Mapping to NIST CSF and 800-53 (continued)

##### Privacy Rule

Our HIPAA Privacy Rule compliance assessment is a comprehensive analysis of an organization’s adherence to all applicable Sections of the Rule, per §45 Code of Federal Regulations (CFR). Our proven approach involves mapping your policies to the Rule’s Sections, assessing your level of compliance following the Office for Civil Rights (OCR) audit protocol, and determining operational compliance.

We will map County’s Privacy Rule policies to applicable HIPAA code sections, as shown below.



##### Breach Notification

As part of our breach notification assessment process, we will determine if the organization is compliant with HITECH standards; policies are aligned with standards; and a breach notification process is in place. The below diagram depicts an effective breach notification process.



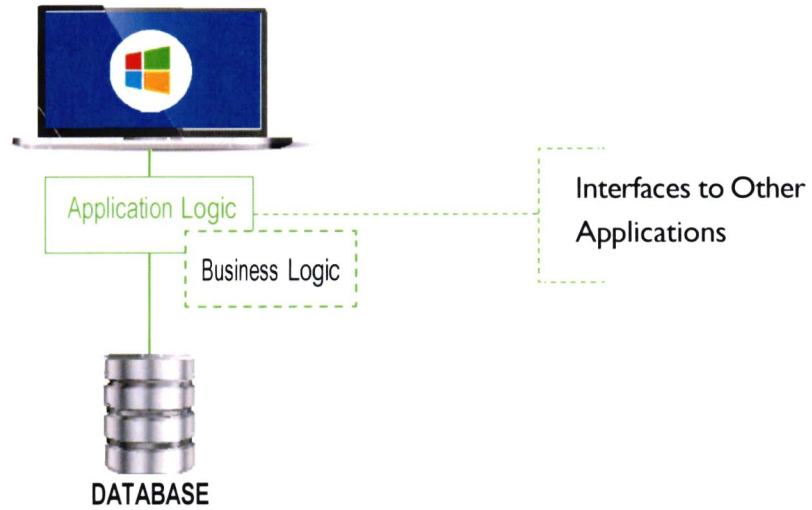
## — Scope of Services

### 1. Vendor Requirements (continued)

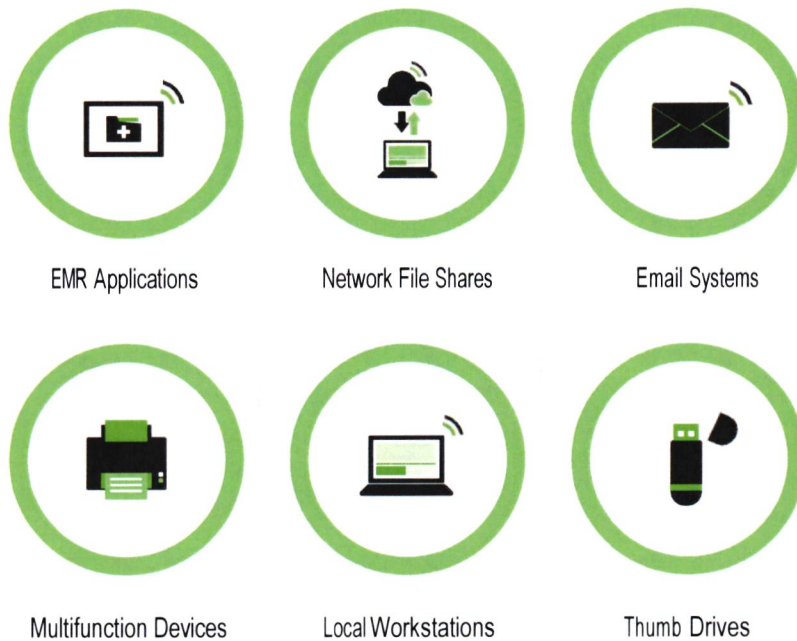
#### HIPAA Security and Privacy Rule Assessment and Mapping to NIST CSF and 800-53 (continued)

#### ePHI Information Assets

Securance has experience assessing Tier I EMR applications. Our evaluation includes:



Securance identifies all areas where ePHI can live, including:



## — Scope of Services

### 2. Technical Network and Security Testing Requirements

Bidders must describe capabilities to meet County of Riverside testing requirements detailed in referenced chart below

Objective/Goals	Description
Network Security Assessment: Provide County of Riverside with a security focused network architecture review, including all networking equipment such as switches, routers, firewall, and etc.	Provides County of Riverside with a security focused network architecture review. Including all networking equipment such as switches, routers, firewalls, etc.
Host/Server Security Assessment: Provides County of Riverside with a security focused host/server architecture review.	Provide County of Riverside with a security focused host/server architecture review.
Endpoint Security Assessment: Provides County of Riverside with an assessment of endpoints/workstations and compare to industry standard and best practices.	Provides County of Riverside with an assessment of endpoints/workstations and compare to industry standard best practices.
Application Security Assessment: Provides County of Riverside with a security assessment of all computer-based applications.	Provides County of Riverside with a security assessment of computer based applications.
Non-Technical Risk Assessment: Provides County of Riverside with an assessment to identify all risks and opportunities that arise from the interactions of a business with its broad range of external stakeholders.	Provides County of Riverside with an assessment to identify all risks and opportunities that arise from the interactions of a business with it's broad range of external stakeholders.

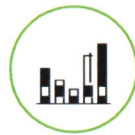
Methodologies for our Network Security, Host | Server Security, Endpoint Security, and Non-Technical Risk Assessments can be found on pages 30-47.



**Firewall Configuration Review**



**Router | Switch Configuration Review**



**Virtual Private Network (VPN) Review**



**Intrusion Prevention | Detection System Assessment**



**Network Architecture Review**



**External Network Vulnerability Assessment and Penetration Test**



**Internal Vulnerability and Penetration Testing**



**Indicators of Compromise Testing**



**Endpoint Security Review**



**Social Engineering | User Security Awareness Training Review**



**Application Security Testing**



**Web Application Testing**

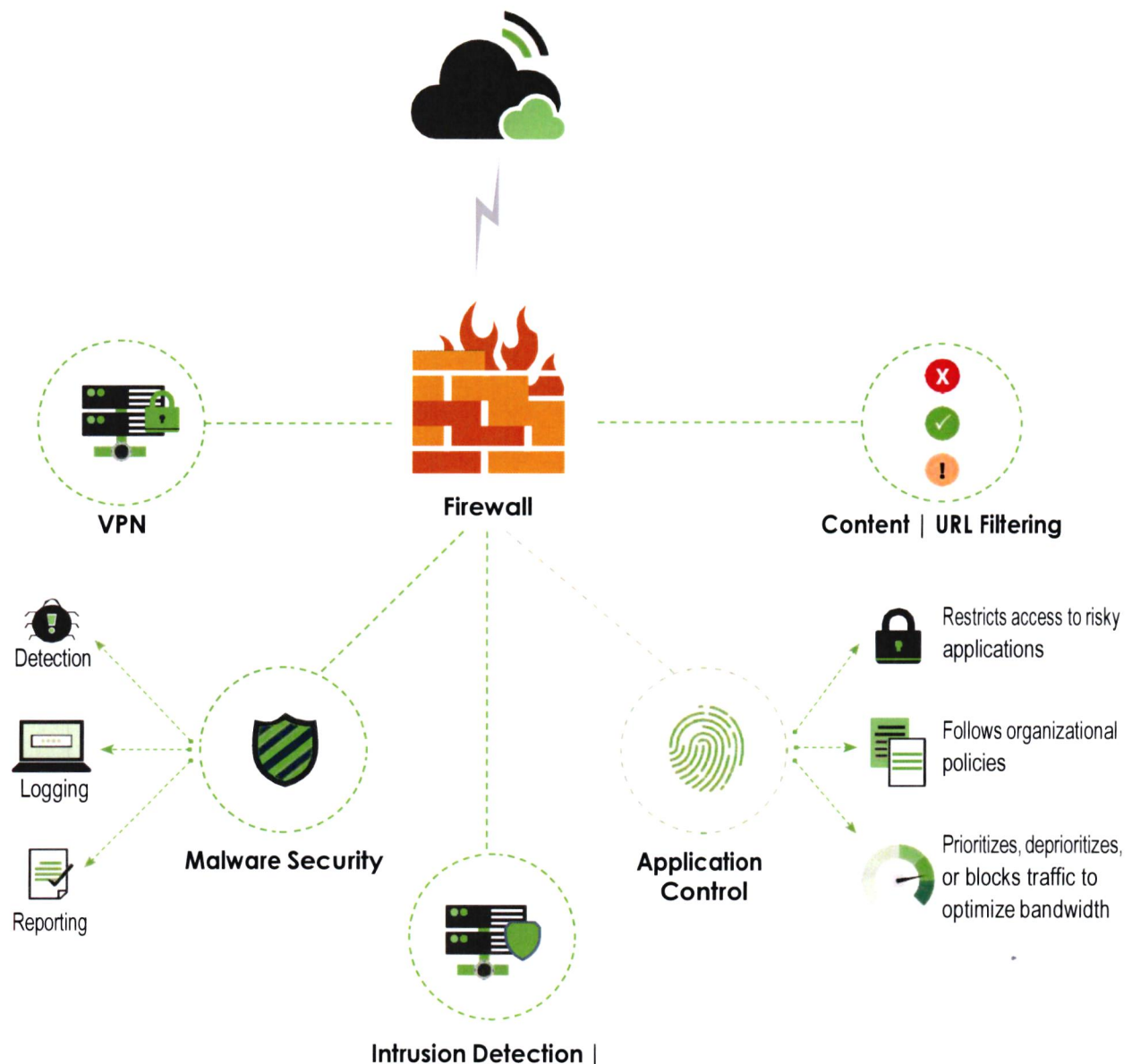
## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Next-Generation Firewall Assessment

Next generation firewalls (NGFW) are complex devices that provide all-in-one network protection via multiple security applications and technologies in one solution. They are managed by sophisticated rules that require regular review and updates to function effectively.

Securance’s approach to performing NGFW configuration reviews covers misconfigurations, vulnerabilities, and other weaknesses that could leave an organization susceptible to attack. Our comprehensive assessment includes evaluations of the modules below.



## — Scope of Services

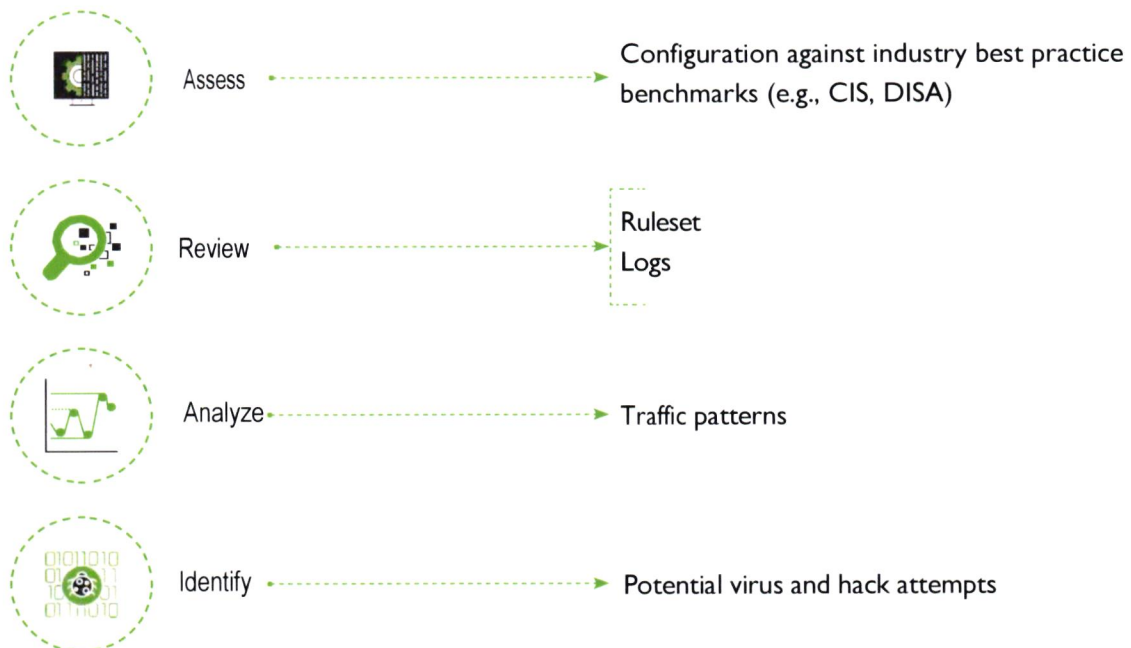
### 2. Technical Network and Security Testing Requirements (continued)

#### Next-Generation Firewall Assessment (continued)

We will ensure:



We will evaluate the configuration of the NGFW, ensuring it aligns with County's network environment and security goals, including:



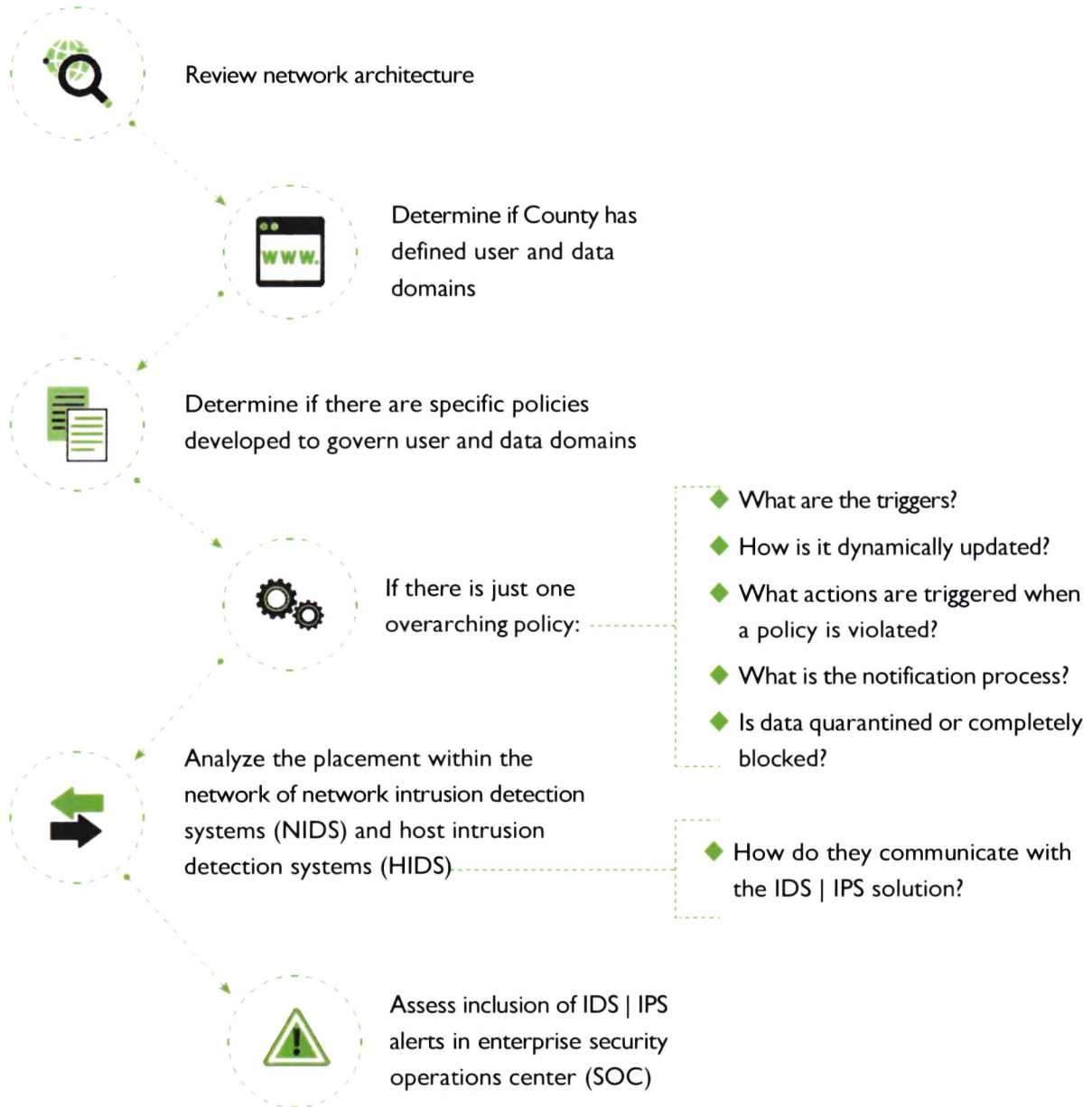
## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Next-Generation Firewall Assessment (continued)

An important part of the NGFW is the intrusion detection and prevention system, which analyzes network traffic and protocol packets for known cyber attack signatures.

Our Process for assessing IDS | IPS is as follows:



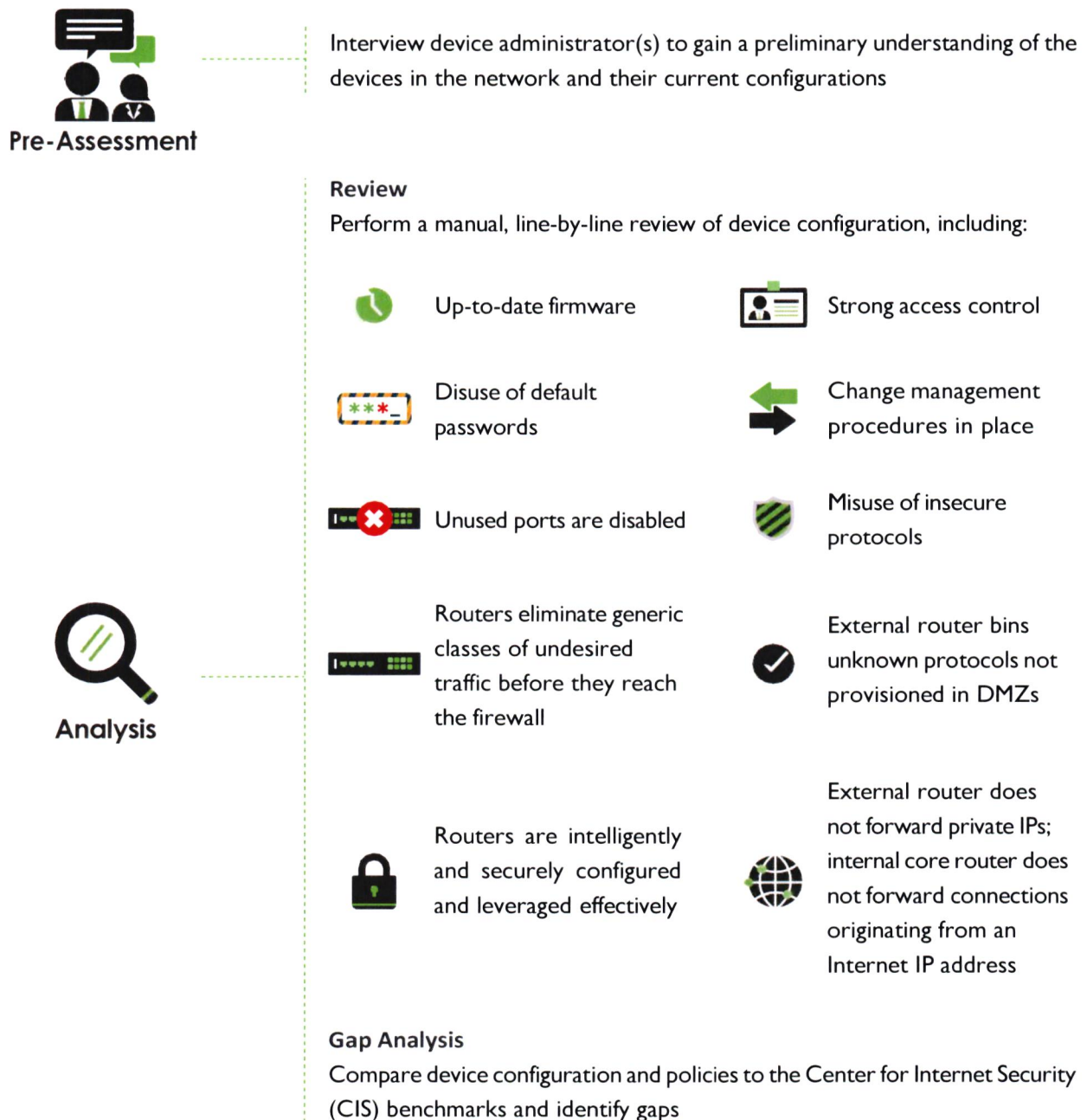
## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Router | Switch Configuration Review

The Securance methodology for evaluating the security of network devices, such as routers and switches, focuses on ensuring these components are correctly configured and are creating and maintaining a secure network devoid of infrastructural gaps.

#### Our Process





## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Virtual Private Network (VPN) Remote Access Assessment

VPNs ensure that the information being transmitted by devices is known only to authorized users. This data is secured by either IPSec or SSL encryption. IPSec connections are designed to have a pre-shared “key” on both the end-user’s device and server so that data can travel securely between both. SSL connections use public key cryptography that creates a secure connection after exchanging encryption keys. Each type of encryption suffers from vulnerabilities that make connections less secure.

#### Our Process



## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Virtual Private Network (VPN) Remote Access Assessment (continued)



#### **Log Monitoring**

We will review the logs using manual and automated techniques to verify that:

- ◆ Logging for security events is enabled
- ◆ Logs are housed in a central location
- ◆ Sensitive information is not logged, e.g., passwords
- ◆ Logs are not altered
- ◆ Alerts are set up
- ◆ Logs are aggregated with other technology logs
- ◆ Logs are reviewed on a regular basis



#### **VPN Policy Ruleset Review**

We will evaluate County's access and policy ruleset to:

- ◆ Verify policies' cybersecurity strength
- ◆ Identify gaps and | or misconfigurations
- ◆ Ascertain if any policies are missing
- ◆ Identify extraneous policies
- ◆ Determine if authentication mechanisms are viable, strong, and appropriate
- ◆ Confirm that capacity and server | appliance load is appropriate | adequate

## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

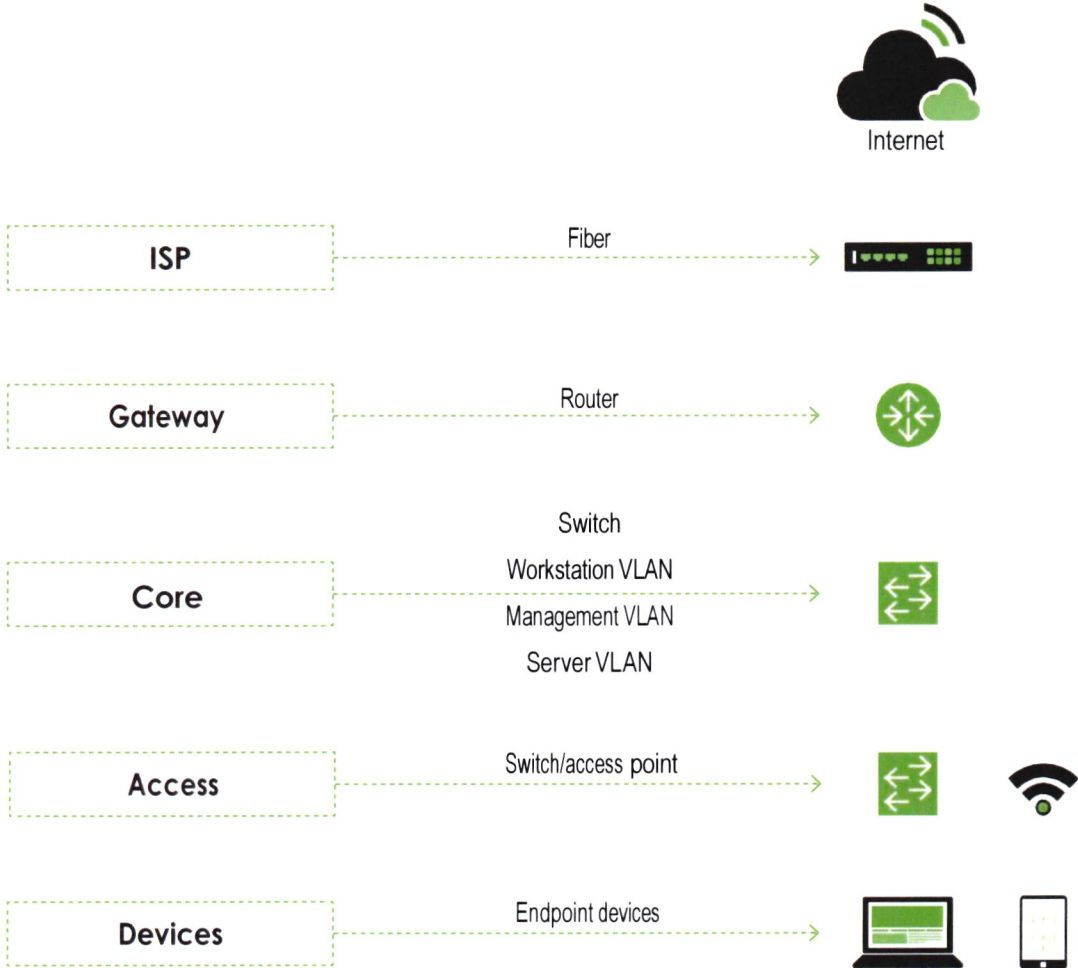
#### Network Architecture Review

Securance ensures the design and architecture of a core network provides bandwidth in the most secure manner possible, without decreasing availability or quantity. In our opinion, the best network design is the one that is secure and meets the needs of its users. There is no one “correct” switched network design. There are only proven design principles that should be incorporated.

Designs can differ based on several real-world factors (e.g., budgets, existing hardware, application requirements, implementation timelines). Our approach starts with gaining an understanding of the network and user requirements, then weighing the pros and cons of each design principle against the overall goals for the design.

Current practices recommend a Layer 3 | 4 switched network. Our analysis includes a review of all three layers and the configuration sets (i.e., switching and routing) at each layer.

A best practice network design models the following:

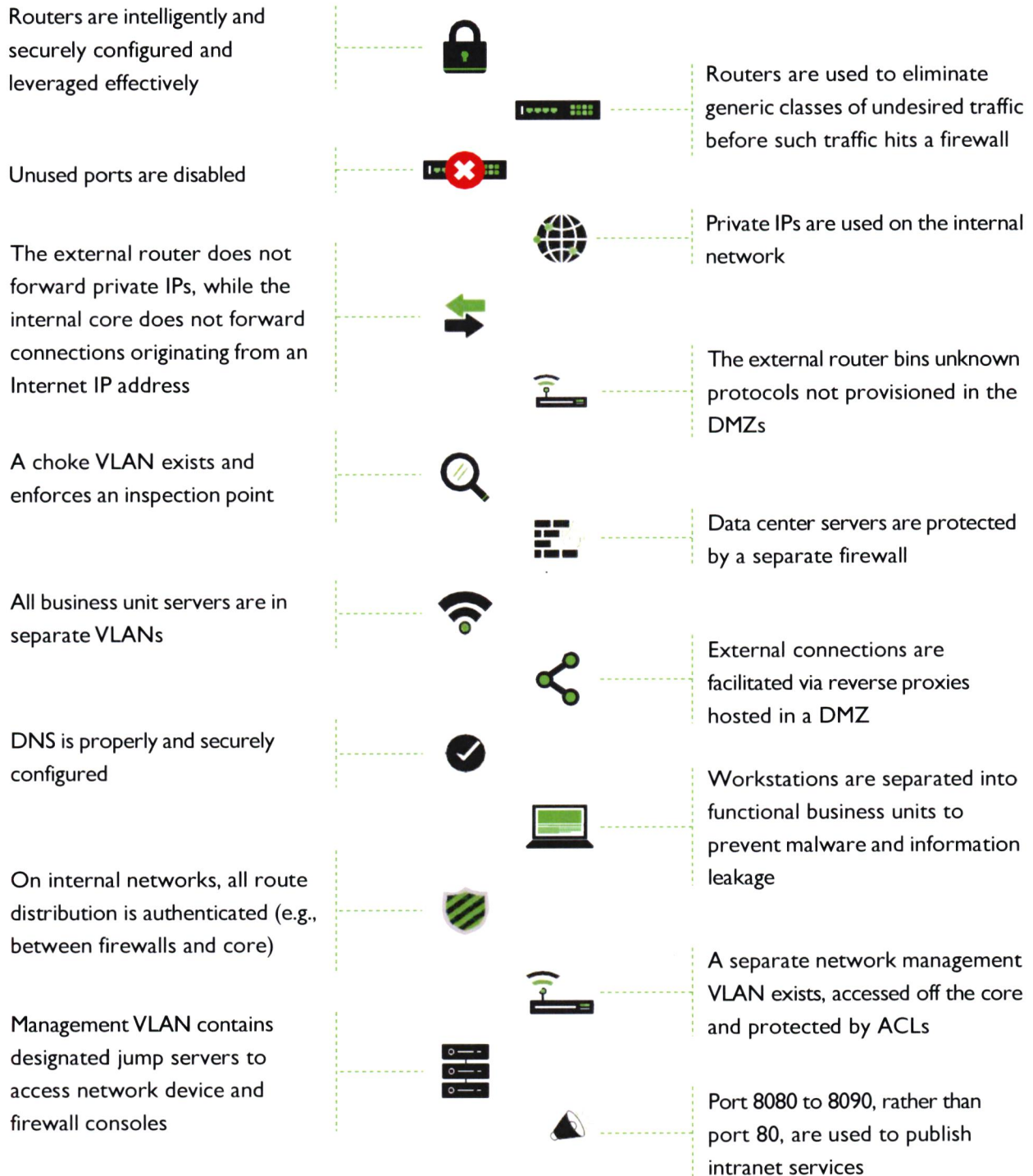


## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Network Architecture Review (continued)

During our assessment, we will evaluate the design of the network, including the below critical components. Our review items are subject to change based on County's specific needs and technologies (e.g., device brand, model, and version).



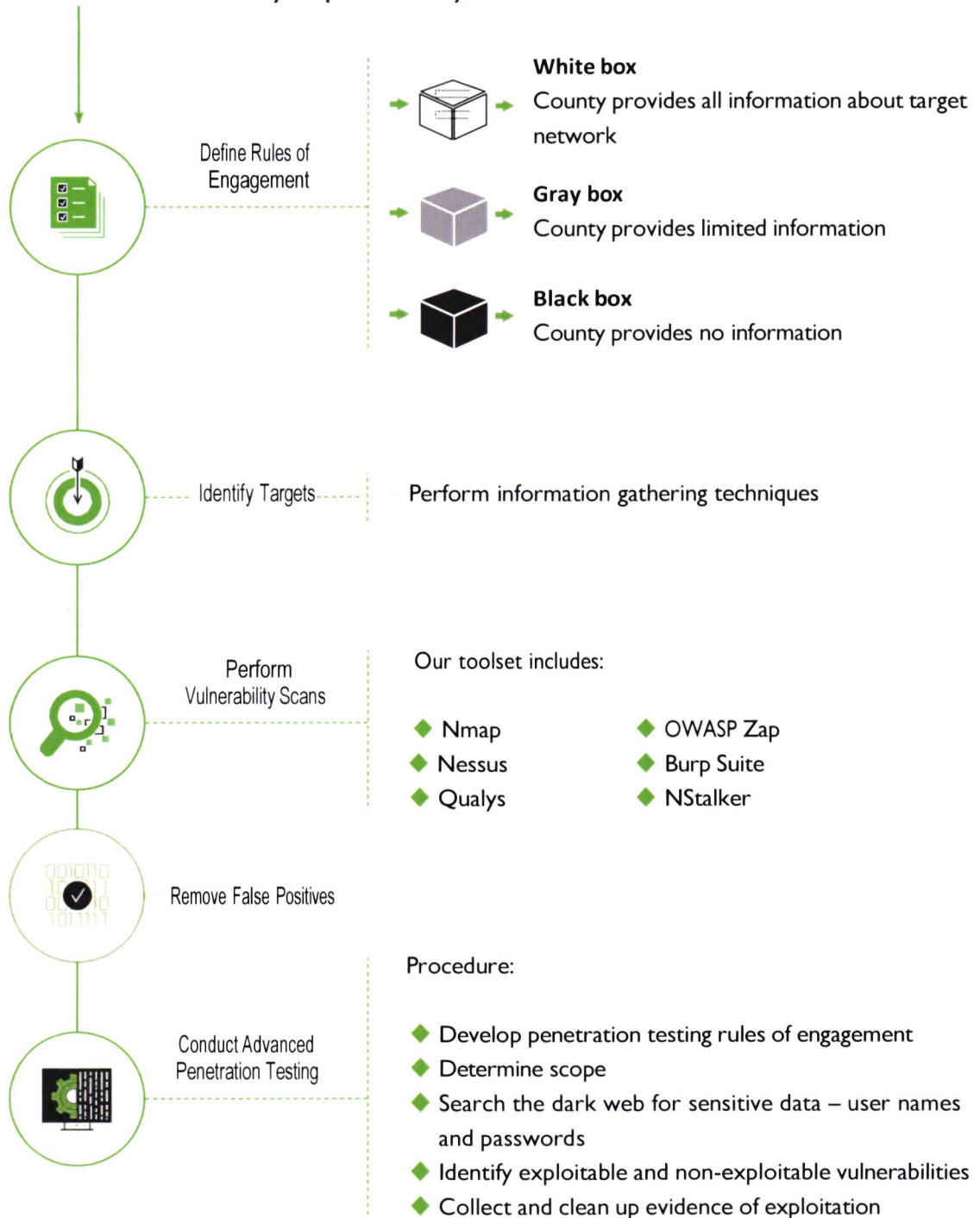
## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### External and Internal Network Vulnerability Assessment and Advanced Penetration Test

Our External and Internal Network Vulnerability Assessment is aligned with industry-leading frameworks, such as NIST SP 800-115, ISSAF, OSSTMM, and OWASP.

#### Securance communicates every step of the way

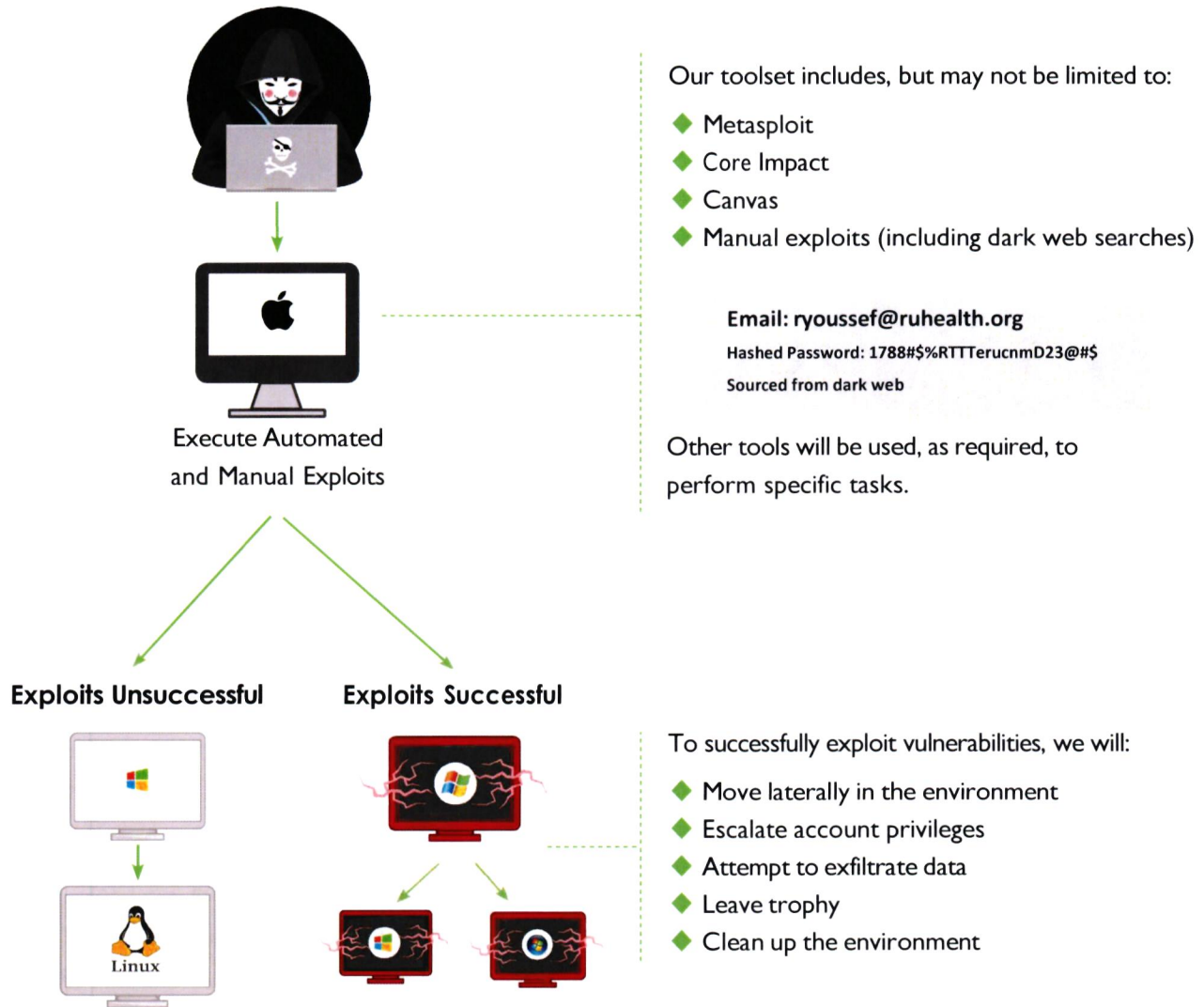


## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

External and Internal Network Vulnerability Assessment and Advanced Penetration Test (cont.)

#### Securance's Ethical Penetration Testing Process



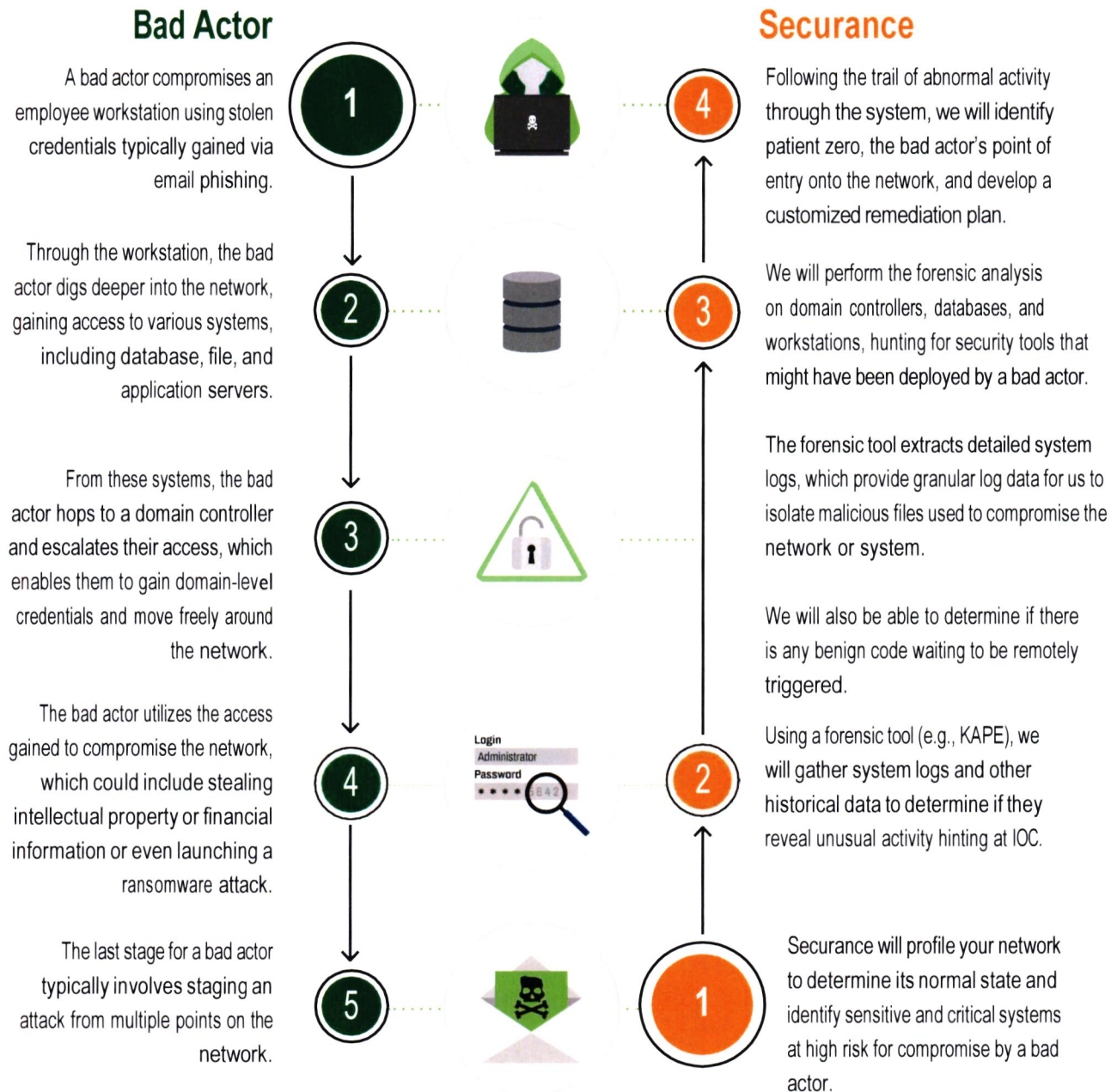
## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Indicators of Compromise Assessment

Indicators of Compromise (IOC) are digital evidence that indicate the potential presence of malicious activity, whether an attack has already occurred or will occur. Identifying IOC informs an organization of network breaches and which security components must be strengthened to deter future incidents.

The below diagram depicts Securance’s comprehensive process for determining instances of network compromise and completing a forensic analysis to identify IOC. We provide an example of how a bad actor might compromise an organization and how we work backward through the breach to determine the original compromised host, or patient zero.

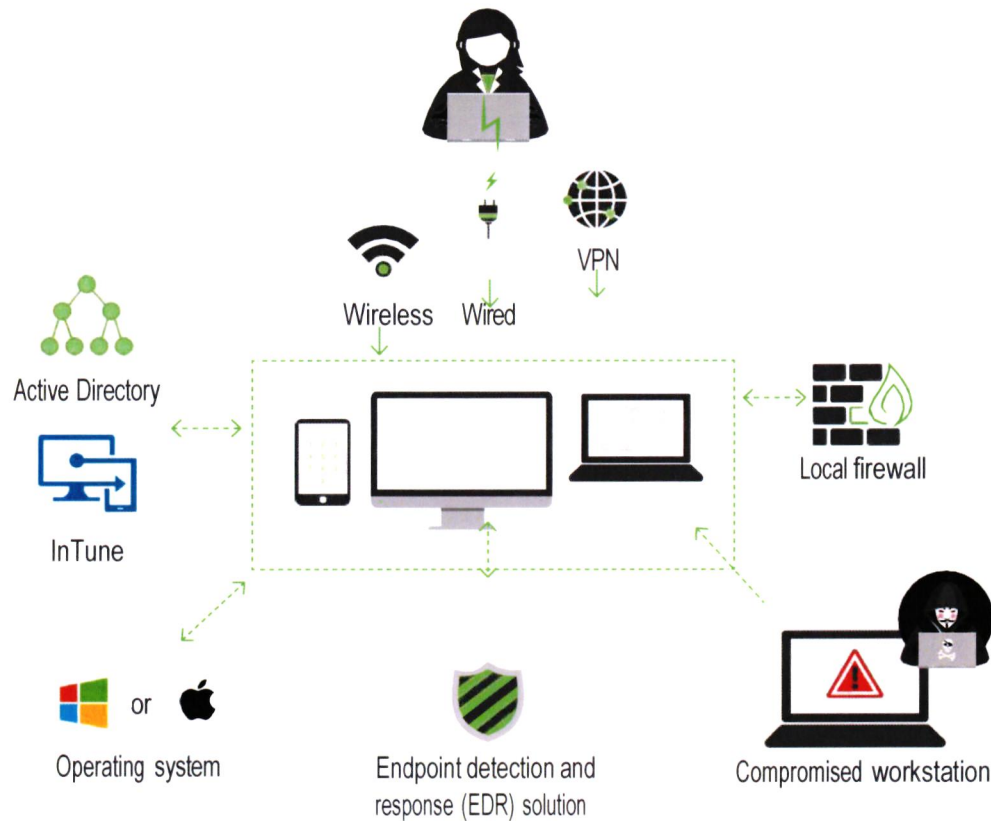


## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Endpoint Configuration Review

Securance’s workstation configuration review examines the overall configuration of endpoint devices and takes a deeper dive into specific device settings and controls to ensure the reliability and security of your IT environment. Effective workstation hygiene reduces the chance of an attacker gaining access to enterprise data and potentially compromising the entire network.



#### Our Approach

- ◆ Gain an understanding of how the endpoint’s security is governed, such as Active Directory Group Policy Objects (AD GPO) or InTune
- ◆ Review the configuration of either the GPO or InTune
  - Assess domain structure and policies
  - Evaluate user and computer attributes
 Or
  - Assess the structure and use of InTune
  - Review policies (e.g., compliance, conditional access)
- ◆ Assess the local security-related configuration options (e.g., BitLocker, enabled firewall)



## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Endpoint Configuration Review (continued)

- ◆ Assess the security posture of the endpoint's underlying operating system and compare it to industry standards and Center for Internet Security (CIS) benchmarks:
  - Establish secure configurations
  - Maintain secure images
  - Deployment management tools
  - Monitoring of configuration management changes
  
- ◆ Assess the effectiveness of the implemented endpoint detection and response (EDR) solution
  - Does it reduce the time required to detect and respond to threats?
  - Does it reduce security operational costs?
  - Is the solution flexible enough to incorporate new findings outside of core forensic evidence (e.g., file system metadata, account activity)?
  
- ◆ Attempt to compromise the workstation by loading malware, visiting malware sites, and performing other simulated attacks, such as permissions escalation, to reach exponentially more sensitive data on the network

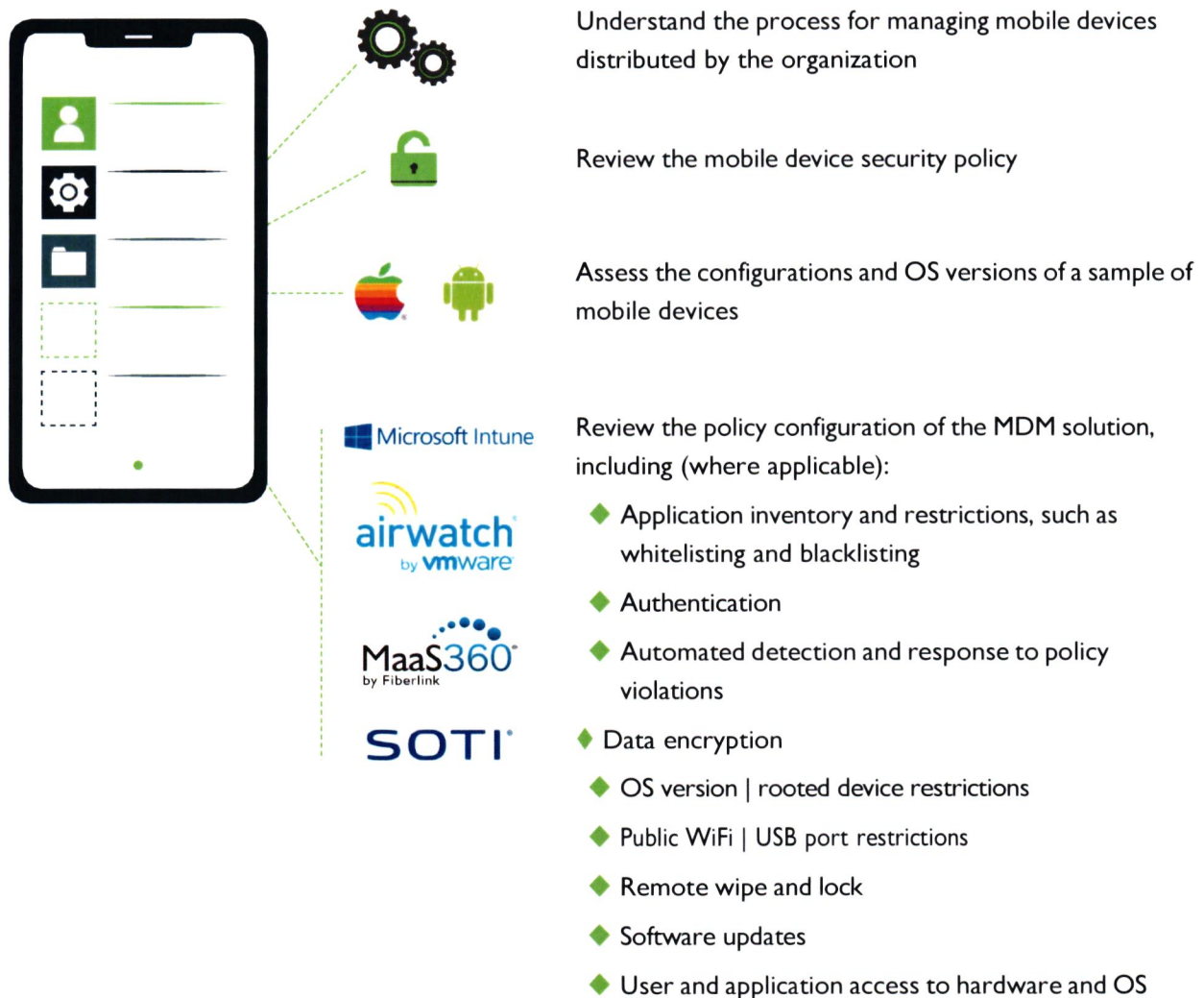
## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Mobile Device Security Assessment

When assessing an enterprise mobile device deployment, Securance reviews the mobility management process, operating system (OS) security, and mobile device management (MDM) solution.

#### Our Process



## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Social Engineering and User Security Awareness Training Review

To decrease the chances of avoidable cybersecurity incidents, County employees should receive both onboarding and annual security training. Training programs should be targeted to the specific audience to be trained such that the appropriate subject matter expertise is delivered to any of three distinct user groups, including: standard end users, system administrators, and managers.

To determine if County’s personnel are receiving adequate training, Securance will select a representative sample of staff from each of the three target groups specified above and:

- ◆ Conduct interviews
- ◆ Conduct tests and simulate security events to verify levels of cybersecurity knowledge and determine if responses are appropriate | adequate
- ◆ Solicit employee feedback to determine if staff feel they are receiving adequate | appropriate training

Based on the results of the training and awareness audit, Securance will provide a remediation plan that highlights severe vulnerabilities in the training program that put County at risk with anticipated remediation effort and costs.

Samples of testing scenarios include:

- ◆ Phishing
- ◆ Smishing
- ◆ Vishing
- ◆ Whaling
- ◆ Spear Phishing
- ◆ Physical Security:
  - Tailgating
  - Diversion Testing
  - Workspace Observance
  - Workstation Inactivity Access



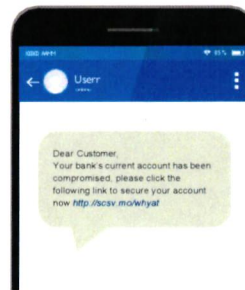
The company appreciates your patience and dedication working from home in the COVID-19 environment. As a token of our appreciation, we are offering all employees discounts at local retail stores, including, but not limited to, those listed below.

Thank you again for all your hard work!



And many other local favorites!

To participate in these savings and have priority access to future offerings, please [click here](#) to register.



## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Application Security Testing

Securance’s methodology for assessing enterprise applications includes analyses of the presentation, application, database, and operating system layers and the IT general controls that govern the environment.

#### ● Presentation Layer

As most current applications are browser-based, either Internet or intranet-facing, our testing approach follows OWASP standards. It includes unauthenticated and authenticated testing and manual and automated procedures.

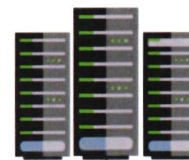


Tools used:

- ◆ Burp Suite
- ◆ N-Stalker
- ◆ WebInspect
- ◆ OWASP ZAP

#### ● Application Layer

Securance will review configurable application control and tolerance settings. In addition, we will ensure that high-risk functions are restricted to authorized users and reviewed by management.



Application Logic

Business Logic

#### ● Database Layer

Securance will identify weaknesses in database design schema, technical vulnerabilities, and entry points through which unauthorized users could gain direct access to the database to extract or insert data.



DATABASE

Our API assessment includes:

- ◆ Evaluating the security of both ends of the API connection
- ◆ Performing manual manipulation
- ◆ Determining data integrity

Via API

Tools used:

- ◆ OWASP ZAP
- ◆ Burp Suite



Enterprise Application Database

Tools used:

- ◆ Application Detective
- ◆ Nessus Pro
- ◆ Manual procedures

## — Scope of Services

### 2. Technical Network and Security Testing Requirements (continued)

#### Application Security Testing (continued)

#### ● Operating System Layer

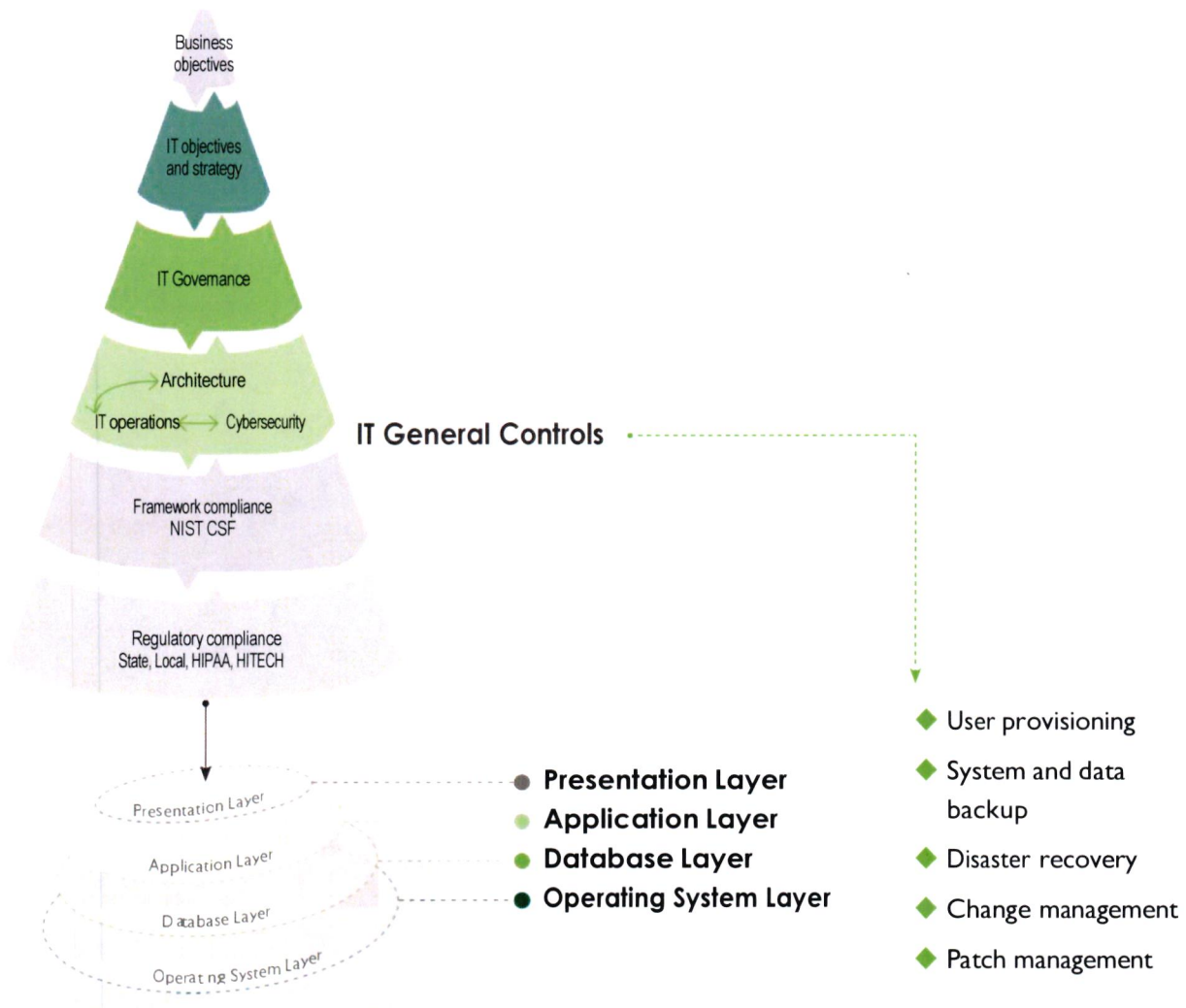
We will evaluate each server operating system (OS) that hosts a presentation layer, application layer, and database layer for:

- ◆ OS-level vulnerabilities
- ◆ Configuration aligned with County’s standards and best practices



#### IT General Controls

We will assess the IT general controls supporting the application environment and compare them to NIST CSF.



## — Scope of Services

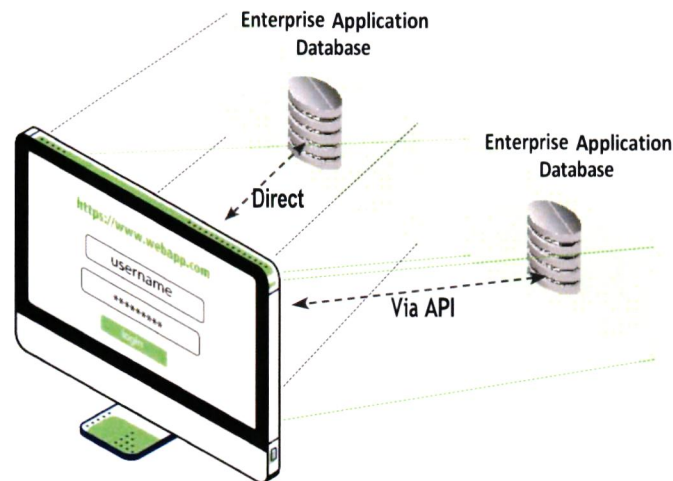
### 2. Technical Network and Security Testing Requirements (continued)

#### Application Security Testing (continued)

Our web application security assessment follows the OWASP Top 10 and includes identifying vulnerabilities at various layers across websites, intranets, extranets, portals, and other web-based services.

We will perform an in-depth analysis, concentrating on the following security related issues:

- ◆ Boolean parameter tampering
- ◆ Broken access control
- ◆ Broken authentication and session management
- ◆ Buffer and integer overflow
- ◆ CGI attacks
- ◆ Common HTTP device attacks
- ◆ Cross site request forgery
- ◆ Cross site scripting (XSS)
- ◆ Directory | file traversal
- ◆ Failure to restrict URL access
- ◆ Format string
- ◆ Generic HTTP attacks
- ◆ Information leakage and improper error handling
- ◆ Injection flaws (e.g., SQL, CRLF)
- ◆ Insecure communications
- ◆ Insecure components
- ◆ Insecure cryptographic storage
- ◆ Insecure deserialization
- ◆ Insufficient logging and monitoring
- ◆ Malicious file | remote execution
- ◆ Microsoft CGI attacks
- ◆ Microsoft IIS attacks
- ◆ Parameter deletion
- ◆ PHP file include
- ◆ Security misconfiguration
- ◆ Sensitive data exposure
- ◆ Special parameter addition
- ◆ XML external entity



### Manual Testing

To detect vulnerabilities that may be missed by automated tools, Securance will perform manual testing, including:

- ◆ URL manipulation
- ◆ Input field character testing
- ◆ Input field string sanitization testing
- ◆ Remote site return validation
- ◆ Software version vulnerability testing

## — Scope of Services

### 3. Security Risk Assessment

In this area, vendor will acknowledge and provide experience of requirements below.

1. All Riverside County Hybrid Entity Departments which include the following approximate IT assets:
  - a. 20,000 users
  - b. 22,000 end-point devices
  - c. 1,000 servers (virtual and physical)
2. Work on-site with Information Security staff members, including physical/security inspection for some facilities.
3. Review current security practices on network infrastructure (switches/routers), physical/virtual servers, firewall, IDS, cloud-based services, and users' accesses.
4. In-person review of the findings with County of Riverside (County and RCIT) Information Security Offices.
5. Review of policy and procedural documentation to ensure information is up-to-date and in alignment with current information security rules, regulations, laws, and best business practices.
6. Analyze security posture in comparison to the National Institute of Standards and Technology (NIST) Cyber Security Framework mapped to HIPAA Security Rule as dictated by HHS.
7. Provide one-time Executive summary report with findings and recommendations for mitigations and best practices.

Please see pages 49-54 for descriptions of our Security Risk Assessment process, including assessments of physical security, network infrastructure (switches/routers), physical/virtual servers, firewall, IDS, cloud-based services, and users' accesses, and policies and procedures. See pages 19-21 for our final reporting and presentation process. See pages 23-28 for a description of our NIST CSF and 800-53 mapped to HIPAA Security Rule assessment process.



**On-Site Physical Security Review**



**Virtual Host Server Security Configuration Assessment**



**Server Configuration Assessment**



**Cloud-Based Services Assessment**



**IT Policy, Procedure, Standards, and Guidelines Review**

## — Scope of Services

### 3. Security Risk Assessment (continued)

#### On-Site Physical Security Inspection at Specified County-MC Facilities

Securance will ensure that your physical security controls protect information assets from environmental threats, human intruders, and the damage caused by supply system failures (i.e. loss of power, Internet, climate control, or any other infrastructure provider).

Our physical security review includes the following activities:



#### Information Gathering

- ◆ Review physical security policies and procedures
- ◆ Interview personnel responsible for physical security



#### Risk and Vulnerability Identification

- ◆ Perform a walkthrough of the facility | data center
- ◆ Review site selection, considering environmental risks and compliance requirements
- ◆ Evaluate physical and environmental security controls, including:
  - Access controls and perimeter defenses
  - Surveillance and monitoring mechanisms
  - Destruction and sanitization procedures for storage devices
  - Location of information systems components, wiring, and cabling
  - Incident management, reporting, and response procedures
- ◆ Physical security awareness training



#### Analysis

- ◆ Compare physical security measures to best practices and regulations
- ◆ Identify risks, vulnerabilities, and opportunities for improvement



## — Scope of Services

### 3. Security Risk Assessment (continued)

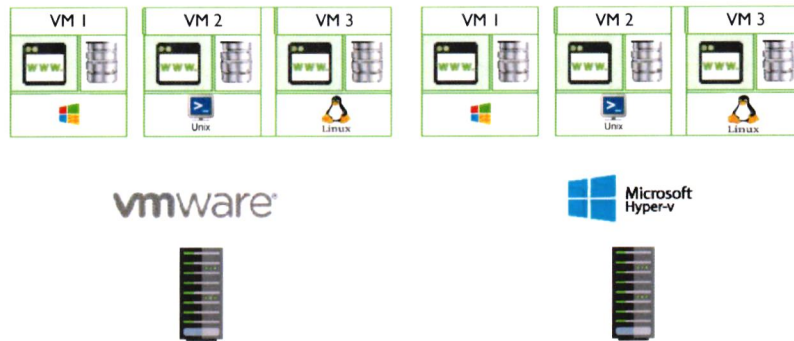
#### Virtual Host Server Security Configuration Assessment

Securance’s methodology for assessing virtual server security includes reviews of operating system (OS) configurations and governing general computing controls.

#### Our Process

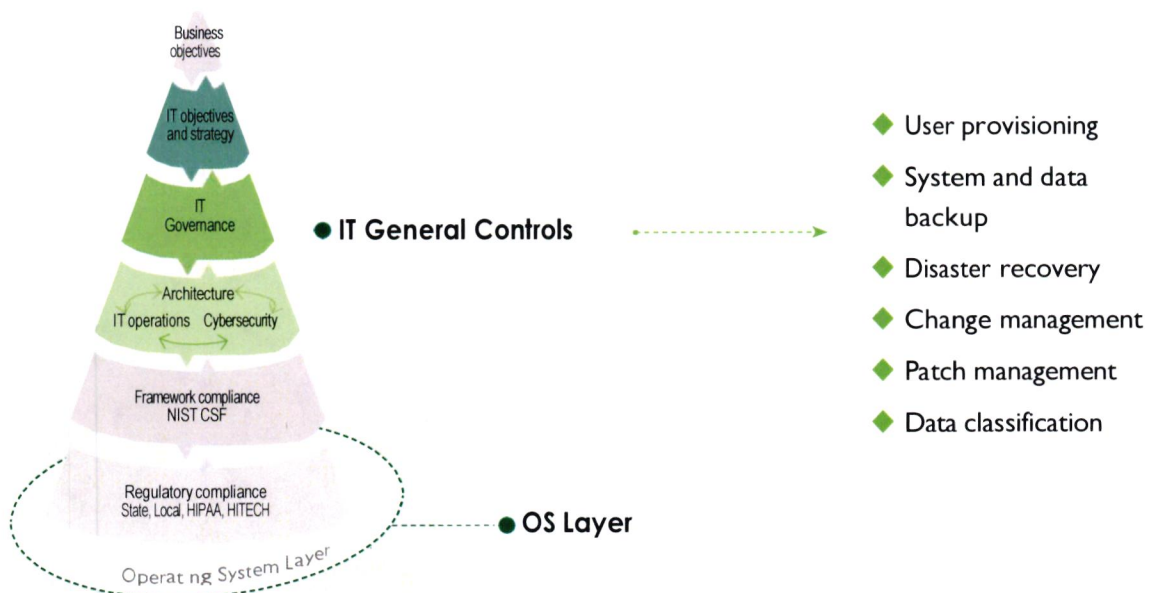
Our comprehensive review will include:

- ◆ Identification of hypervisor vulnerabilities
- ◆ Analysis of virtual host configuration
- ◆ Analysis of network architecture (e.g., segmentation of virtual machines (VMs), prevention of single points of failure)
- ◆ Review of templates for deploying new VMs
- ◆ Configuration review aligned with CIS, DISA, and | or vendor benchmarks and hardening standards
- ◆ Configuration comparison to the City’s internal standards



#### IT General Controls

We will assess the IT general controls supporting the server environment and compare them to NIST CSF.



## — Scope of Services

### 3. Security Risk Assessment (continued)

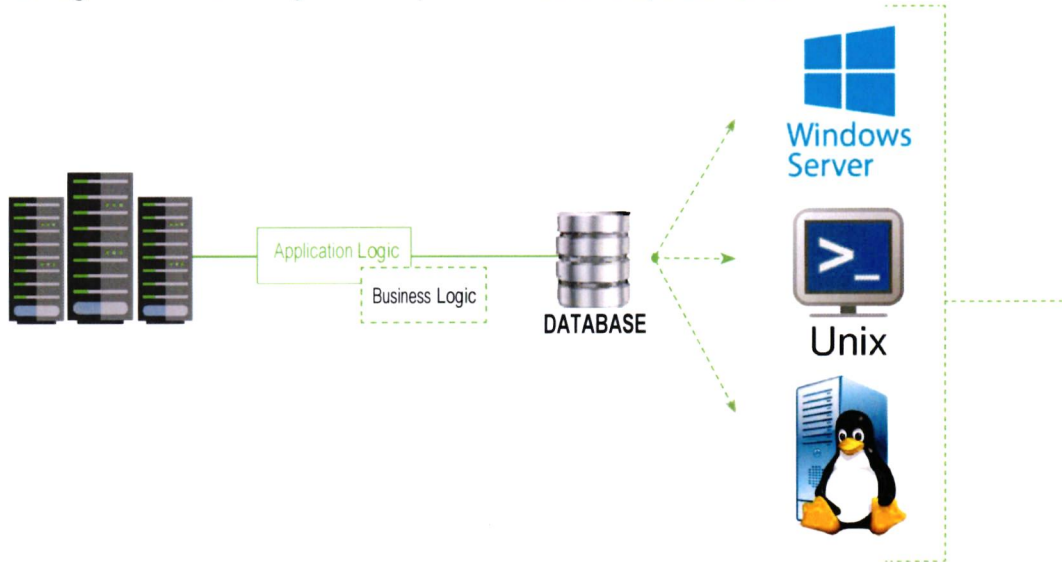
#### Server Configuration Assessment

Securance’s methodology for assessing server security includes reviews of operating system (OS) configurations and governing general computing controls.

#### Operating System Layer

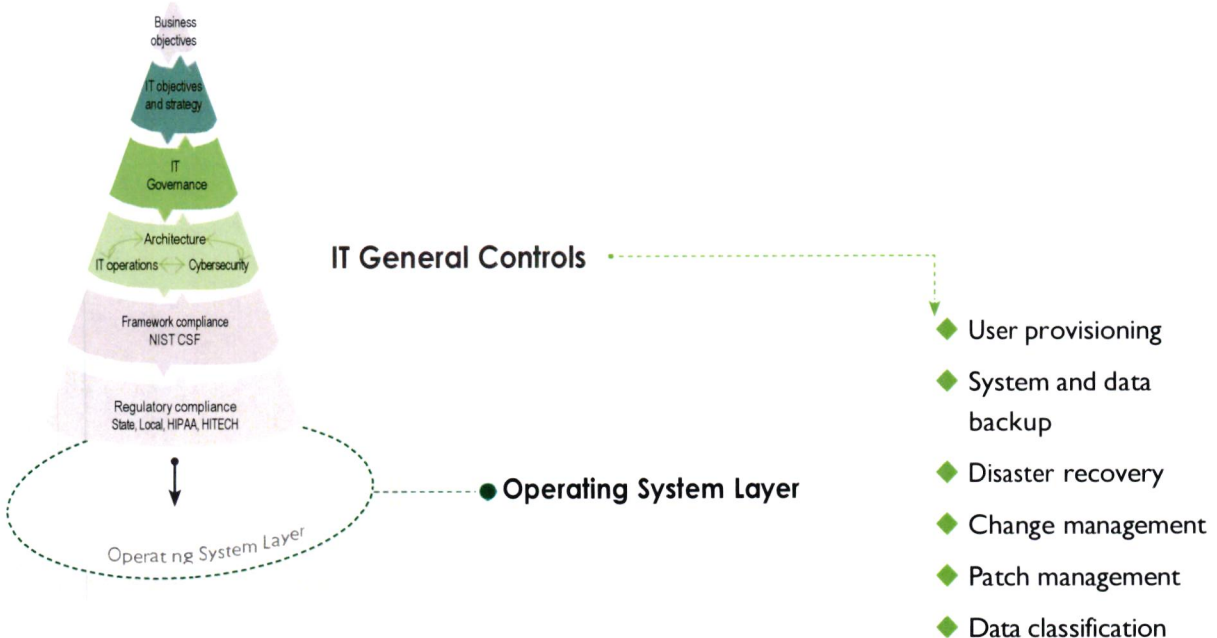
● We will evaluate each server OS for:

- ◆ OS-level vulnerabilities
- ◆ Configuration assessed against CIS and/or DISG Standards
- ◆ Configuration assessed against best practices and County’s standards



#### IT General Controls

We will assess the IT general controls supporting the server environment and compare them to NIST CSF..



## — Scope of Services

### 3. Security Risk Assessment (continued)

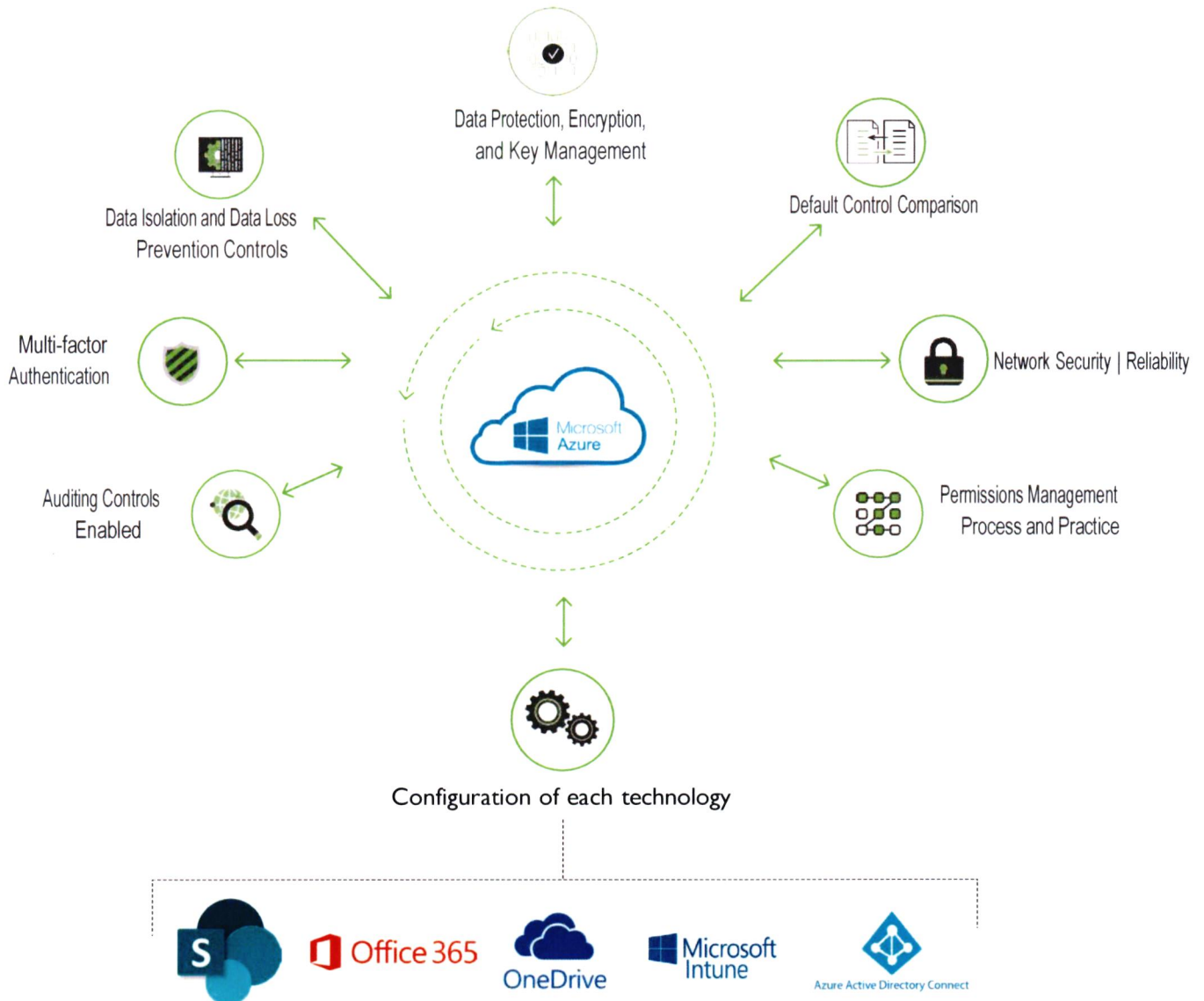
#### Cloud-Based Services Assessment

County did not define what cloud services, infrastructure, or applications would be in scope for the cloud-based services assessment. Therefore, we provide our methodology for assessing a popular cloud provider, Microsoft Azure, as an illustrative example of our approach to cloud security assessments.

Securance has direct experience evaluating the implementation of Microsoft cloud-service applications by reviewing how these applications are configured relative to client configurable controls and assessing them against best practices.

Our methodology aligns with information security best practices, regulatory requirements, and the latest standards for cloud computing in software as a service (SaaS) cloud delivery and deployment models.

We will assess the following common control domains and security configurations in County’s environment:



## — Scope of Services

### 3. Security Risk Assessment (continued)

#### IT Policy, Procedure, Standards, and Guidelines Review

Our methodology for assessing IT policies and procedures addresses all common components of an IT organization.

#### Securance:



**Defines** a policy as management's intentions relative to mitigating a risk. Policies should be supported by detailed procedures that provide policy implementation guidance to IT engineers and administrators.



**Does not** support procedural language embedded in policy language, or policies for the sake of policies. We will understand County's organization and right-size each document to suit County's needs and IT environment specifically.

#### Our process includes:



Gaining an understanding of County's daily IT operations



Reviewing existing, or draft new, policies that map to day-to-day operations

- ◆ Conducting IT process owner interviews
- ◆ Determining gaps in policies, procedures, and standards
- ◆ Drafting policies customized to County's IT environment
- ◆ Reviewing draft policies with IT process owners



Mapping policies to desired security and control frameworks

- ◆ Reviewing draft policies with IT process owners to ensure each policy maps to daily activities



Implementing new policies by training IT staff to adhere to them

## — Scope of Services

### 3. Security Risk Assessment (continued)

#### IT Policy, Procedure, Standards, and Guidelines Review (continued)

To ensure County's policies and procedures are comprehensive, accurate, and effective, Securance will evaluate them for the criteria below or develop policies or procedures that contain these criteria.

Criteria	Definition
Overview	Summary of the need for the policy
Scope	Devices, data, documents, or systems covered under the policy
Purpose	Overall objective of the policy
Policy	A measure by which an organization conducts a process; may be aligned to a particular framework
Disciplinary Action	Defined actions the organization will take in the event of a failure to comply with the policy
Definitions	A table of definitions for terms used within the policy
Exceptions	Any circumstances under which the policy would not apply
Expected Impact	Projected outcome of maintaining and implementing the policy
Revision History	A table denoting when the policy was last updated and what areas were modified
Approval	Process for formally instating the policy and the party responsible for approval

## — Scope of Services

### 4. Data and Application Security

Does the Vendor have its own data security and application security management system to safeguard County of Riverside operational files and patient data? Provide a list of security certifications you hold.

Securance uses Box.com as a secure document sharing portal. The data is encrypted in transit using high strength TLS encryption and at rest via 256-bit AES encryption. All engagement work papers will be digitized, encrypted, and stored on a secure file server. County's PM may direct Securance to destroy all work papers after an electronic copy has been delivered to the designated personnel. Securance will not store any patient data over the course of the project.

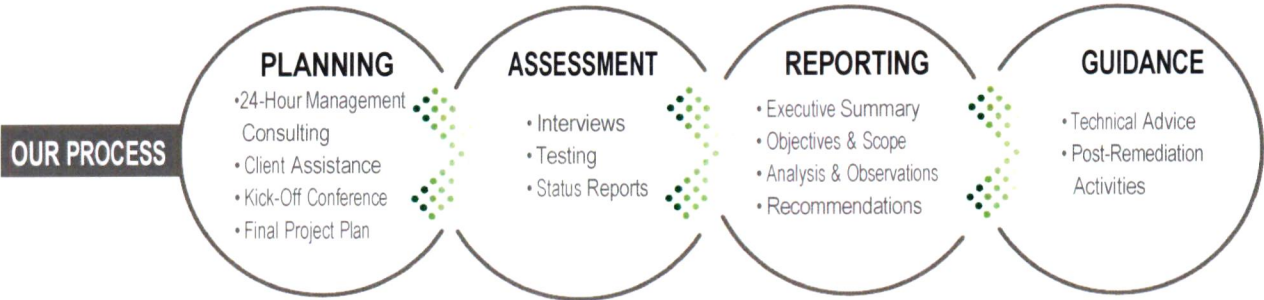
We hold a number of security certifications that are relevant to the scope of this project, including:

- + CEH - Certified Ethical Hacker
- + CCSP - Certified Cloud Security Professional
- + CHP - Certified HIPAA Professional
- + CDSPE - Data Privacy Solutions Engineer
- + CISM - Certified Information Security Manager
- + CISSP - Certified Information Systems Security Professional
- + CompTIA A+, Network+, Linux +, Security+ Certification
- + HCISPP - Healthcare Information Security and Privacy Practitioner

— Scope of Services

5. Project Approach

I. Describe your proposed approach to include both you and your customer’s responsibilities and timelines?



Securance is dedicated to performing this engagement as efficiently as possible. Paul Ashe, your engagement manager, will be responsible for ensuring project success by facilitating regular communication and providing status reports that will track project progress, possible project risks, and other information pertinent to the project.

**Engagement Manager**

**Paul Ashe**, CISA, CISSP, CPA, HCISPP (pending), CMMC-AB RP (pending)

Paul will manage the Securance team, keep County’s project manager (PM) updated on project status, and notify County of any potential concerns or issues. He will also oversee:

- ◆ Development of detailed assessment procedures based on County’s environment
- ◆ Execution of the information security risk assessment in an efficient manner
- ◆ Identification of risks, vulnerabilities, compliance gaps, and other opportunities for improvement

**Senior IT Security Consultants**

**Ray Resnick**, CISSP, CEH, CCNA, CISM, Security +, CDPSE, CCSP, CMMC-AB RP

**Chris Bunn**, CISSP, CHP, CMMC-AB RP

**Ibrahim Badrawi**, CCNA, CVA, Security +

Ray, Chris, and Ibrahim will work with Paul to:

- ◆ Plan, coordinate, and execute assessment based on County’s environment
- ◆ Identify risks, vulnerabilities, compliance gaps, and other opportunities for improvement
- ◆ Prepare assessment reports, other deliverables, and status reports for review with County’s PM
- ◆ Notify him of any project issues or delays

## — Scope of Services

### 5. Project Approach (continued)

#### County's Responsibilities and Logistics

Securance has made the following assumptions regarding County's responsibilities during this engagement:

- ◆ Securance will have full access to all client participants and personnel, as required to complete the engagement
- ◆ County's personnel will provide all information requested to complete the engagement in a timely manner
- ◆ County's PM will be available to discuss the project's progress with the Engagement Manager
- ◆ County's management will be responsible for all remediation of identified vulnerabilities and risks
- ◆ Securance requires adequate workspace and Internet connections while on site to access email and other resources
- ◆ Securance requires access to a dedicated phone extension and printing capabilities

#### 2. Does your approach include offshore services or support?

Securance will not use offshore services or support in the performance of this project.



— Scope of Services

5. Project Approach (continued)

3. If you are successfully awarded this bid, what is your implementation timeline?

The chart below outlines each step in our risk assessment process, designating major tasks, subtasks, key milestones, and the anticipated task owner. This project plan will be refined during the planning phases of the engagement between Securance and County.

Information Security Risk Assessment Services	Week 1	Week 2	Resource
24 Hour Management Consulting			Paul Ashe County PM
Kick-off Meeting			Paul Ashe County PM
Prepare Client Assistance Memo			SC Consultants
Respond to Client Assistance Request			County Staff
Review Client Assistance Request			SC Consultants
<b>Network Security Assessment</b>			
Firewall Configuration Assessment			SC Consultants
Interview firewall administrator			SC Consultants County Staff
Analyze firewall configuration			SC Consultants
Assess results of configuration analysis			SC Consultants
Intrusion Prevention   Detection System Assessment			SC Consultants
Perform line-by-line review of the IPS   ATD configuration			SC Consultants
Evaluate detection capabilities and actions taken when a malicious event is detected			SC Consultants
Review processes for prioritizing events, sending alerts, tracking   documenting incidents, and data aggregation			SC Consultants
Router   Switch Configuration Assessment			SC Consultants
Interview device administrator			SC Consultants County Staff
Obtain device model and firmware version			SC Consultants
Analyze device configuration file			SC Consultants
Assess results of analysis			SC Consultants

◆ WORK PRODUCT REVIEWS

▼ PROJECT STATUS MEETINGS (held bi-weekly)

## — Scope of Services

### 5. Project Approach (continued)

Information Security Risk Assessment Services	Week 2 ▼ Week 3	Resource
<b>VPN Configuration Assessment</b>		SC Consultants
Interview VPN administrator, review logs and assess IT governance		SC Consultants County Staff
Perform technical scan of VPN appliance		SC Consultants
Assess configuration of VPN		SC Consultants
Perform ITGC assessment of remote access		SC Consultants
Analyze results		SC Consultants
Review with VPN Administrator	▶	SC Consultants County Staff
<b>Network Architecture Review</b>		SC Consultants
Review network design, user requirements, and organizational objectives		SC Consultants
Interview network engineer regarding network architecture		SC Consultants County Staff
Compare current architecture to best-practice design principles		SC Consultants
Review results with network engineer	▶	SC Consultants County Staff
<b>External Network Vulnerability Assessment and Penetration Test</b>		SC Consultants
Perform information gathering of public information		SC Consultants
Perform vulnerability scanning		SC Consultants
Analyze results to remove false positives		SC Consultants
Review results of scan with County	▶	Paul Ashe County PM
Identify hosts to attempt to exploit and confirm with County		SC Consultants
Perform exploit testing		SC Consultants
Extend testing to escalate privileges and move laterally in environment		SC Consultants
Review results with County	▶	Paul Ashe County PM

◆ WORK PRODUCT REVIEWS

▼ PROJECT STATUS MEETINGS (held bi-weekly)

## — Scope of Services

### 5. Project Approach (continued)

Information Security Risk Assessment Services	Week 4	Week 5	Resource
<b>Internal Network Vulnerability Assessment and Penetration Test</b>			
Perform information gathering of public information			SC Consultants
Perform vulnerability scanning			SC Consultants
Analyze results to remove false positives			SC Consultants
Review results of scan with County		▶	Paul Ashe County PM
Identify hosts to attempt to exploit and confirm with County			SC Consultants
Perform exploit testing			SC Consultants
Extend testing to escalate privileges and move laterally in environment			SC Consultants
Review results with County		▶	Paul Ashe County PM
<b>Indicators of Compromise (IOC) Testing</b>			
Profile network, determine normal state behavior, and gather system logs and historical data			SC Consultants
Use forensic tools to identify unusual activity and determine extent of compromise (if one exists) and patient zero			SC Consultants
<b>Host   Server Security</b>			
<b>Virtual Host Server Security Configuration Assessment</b>			
Identify hypervisor vulnerabilities			SC Consultants
Analyze virtual host configuration			SC Consultants
Analyze network architecture			SC Consultants
Review templates for deploying VMs			SC Consultants
Configuration review against CIS benchmarks and County standards			SC Consultants
<b>Server Configuration Assessment</b>			
Assess County's build and configuration standards			SC Consultants
Interview server administrator			SC Consultants County Staff
Perform vulnerability scan of the operating system			SC Consultants
Perform configuration scan and analysis of OS			SC Consultants
Analyze results of scanning			SC Consultants
Review results with server administrator		▶	SC Consultants County Staff

## — Scope of Services

### 5. Project Approach (continued)

Information Security Risk Assessment	Week 5	Week 6	Weeks 7	Week 8	Resource
<b>Endpoint Security Review</b>					
<b>Endpoint Security Review</b>					
Assess endpoint build and configuration standards					SC Consultants
Perform a vulnerability analysis of endpoints					SC Consultants
Assess endpoints' hardened security posture against County's objectives					SC Consultants
Assess endpoints' configuration against NIST CSF benchmarks					SC Consultants
<b>Mobile Device Security Assessment</b>					
Research organizational process for managing mobile devices					SC Consultants
Review mobile device security policy					SC Consultants
Assess configurations and sample OS versions					SC Consultants
Review policy configuration of the MDM solution with County PM					SC Consultants County PM
<b>Social Engineering and User Security Awareness Training Review</b>					
Determine social engineering campaign types and obtain the list of targets					SC Consultants
Perform social engineering techniques					SC Consultants
Determine the value of obtained information and attempt to use it to exploit additional confidential information					SC Consultants
<b>Application Security Assessment</b>					
<b>Application Security Testing</b>					
Gain an understanding of the application in scope					SC Consultants
Review system documentation, technical controls, and security practices					SC Consultants
Interview personnel responsible for security of the application					SC Consultants
Test enterprise application controls					SC Consultants
Review the design and operating effectiveness of supporting IT general controls					SC Consultants
<b>Web Application Security Testing</b>					
Assess the hosting server and associated web server's configurations					SC Consultants
Perform unprivileged web application vulnerability testing					SC Consultants
Perform privileged web application vulnerability testing					SC Consultants
Perform manual web application testing					SC Consultants
Analyze results of all testing					SC Consultants
Review results with application administrator					SC Consultants County Staff

## — Scope of Services

### 5. Project Approach (continued)

Information Security Risk Assessment	Week 8 ▼ Week 9	Resource
<b>Cloud-Based Services Assessment</b>		
Inventory, classify, and analyze organizational data and asset risks		SC Consultants
Examine sensitivity and privacy requirements, compliance needs, and legal obligations		SC Consultants
Review and analyze cloud-relevant documentation		SC Consultants
Conduct technical testing and evaluate security controls		SC Consultants
<b>Non-Technical Risk Assessment</b>		
<b>IT Policy, Procedure, Standards, and Guidelines Review</b>		
Evaluate current policies to ensure they include essential components		SC Consultants
Perform comparative analysis against best practices		SC Consultants
Document and prioritize observations and gaps		SC Consultants
<b>User Access and Provisioning Review</b>		
Gain an understanding of the AD architecture		SC Consultants
Review AD configuration		SC Consultants
Review InTune configuration		SC Consultants
Perform API technical testing		SC Consultants

◆ WORK PRODUCT REVIEWS

▼ PROJECT STATUS MEETINGS (held bi-weekly)

*Remainder of page left intentionally blank.*

## — Scope of Services

### 5. Project Approach (continued)

Information Security-\ Risk Assessment	Week 9 Week 10-12 Week 13-14	Resource
<b>NIST CSF Assessment</b>		
Assess key people, processes, and technologies against NIST CSF to identify control gaps		SC Consultants
Review IT governance documents		SC Consultants
Conduct interviews with relevant IT staff		SC Consultants
Perform gap analysis of current security tier level against NIST CSF		SC Consultants
Develop a current state framework profile		SC Consultants
Develop a NIST CSF roadmap		SC Consultants
<b>HIPAA Assessment and Mapping to NIST CSF</b>		
<b>Privacy Rule</b>		
Obtain and review all HIPAA privacy policies and supporting procedures and forms		SC Consultants
Compare County's policies to required policies		SC Consultants
Interview persons within County with knowledge of the HIPAA privacy policies		SC Consultants County Staff
Perform operational compliance tasks to confirm adherence to privacy policies		SC Consultants
Analyze full results		SC Consultants
<b>Breach Notification</b>		
Obtain and review all HIPAA breach notification policies		SC Consultants
Interview the Privacy and Security Officer		SC Consultants County Staff
Review any prior breach documentation		SC Consultants
Assess the process and technologies in place around breach notification, risk assessment and reporting		SC Consultants
Analyze results of all activities performed		SC Consultants
<b>Security Rule</b>		
Obtain and review all HIPAA Security Rule policies		SC Consultants
Compare County's policies to required policies		SC Consultants
Identify information assets that contain, store, maintain, support or transmit PHI and ePHI		SC Consultants
Perform testing of Administrative, Physical, and Technical safeguards		SC Consultants
Analyze results of all activities performed		SC Consultants
Map Assessment Findings to the NIST CSF		SC Consultants
<b>HITECH Assessment</b>		SC Consultants

## — Scope of Services

### 5. Project Approach (continued)

Information Security-Risk Assessment	Week 15	Week 16	Resource
<b>On-Site Physical Security Inspection</b>			
Review physical security policies   procedures			SC Consultants
Interview physical security personnel			SC Consultants County Staff
Perform walkthrough assessments			SC Consultants
Review site selection and layout			SC Consultants
Evaluate design   operating effectiveness of physical   environmental security controls			SC Consultants
Compare physical security measures to best practice standards   applicable regulations			SC Consultants
Identify risks, vulnerabilities, and opportunities for improvement			SC Consultants
<b>Reporting   Deliverables</b>			
Review and Comparison to June 2017 Security Assessment Report			SC Consultants
Develop Draft Report of Findings and Recommendations and Remediation Roadmap			Paul Ashe SC Consultants
Cybersecurity Posture   Risk Appetite Mapping			SC Consultants
In-person review of the findings with County Information Security Office			Paul Ashe County Staff

◆ WORK PRODUCT REVIEWS

▼ PROJECT STATUS MEETINGS (held bi-weekly)

## — Scope of Services

### 6. Business Continuity and Data Recovery

Vendor must have business continuity and data recovery plans in place to ensure that services can be maintained in case of a disaster or an emergency and that any data loss will be recovered.

I. These plans must be provided to the County of Riverside Information Services department?

Securance has business continuity and data recovery plans, based on best practices and industry standards, in place in the event of an incident. Securance will provide these plans upon award.



## Attachment I

### HIPAA Business Associate Agreement Addendum to Contract

Between the County of Riverside and Securance LLC

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of the Underlying Agreement between the County of Riverside ("County") and Contractor and shall be effective as of the date the Underlying Agreement approved by both Parties (the "Effective Date").

#### RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be created by or made available to Contractor for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Contractor or Contractor creates, receives, maintains, transmits, or has access to PHI and/or ePHI of County, Contractor is a business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity in the same manner that they apply to the covered entity, the additional security and privacy requirements of HITECH are applicable to business associates and must be incorporated into the business associate agreement, and a business associate is liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Contractor as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.
  - A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.
    - (1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Contractor

demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

- (a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- (b) The unauthorized person who used the PHI or to whom the disclosure was made;
- (c) Whether the PHI was actually acquired or viewed; and
- (d) The extent to which the risk to the PHI has been mitigated.

(2) Breach excludes:

(a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.

(b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.

(c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- B. "Business associate" has the meaning given such term in 45 CFR §164.501, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.
- C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.
- D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.
- E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media.
- F. "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given such term in 42 USC §17921(5).
- G. "Health care operations" has the meaning given such term in 45 CFR §164.501.
- H. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.
- I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A and E.
- K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI.

- L. "Required by law" has the meaning given such term in 45 CFR §164.103.
- M. "Secretary" means the Secretary of the U.S. Department of Health and Human Services ("HHS").
- N. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- O. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts A and C.
- P. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- Q. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued under 42 USC §17932(h)(2).

**2. Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.**

- A. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.
- B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum or required by law, in accordance with 45 CFR §164.504(e)(2), Contractor may:
  - 1) Use PHI and/or ePHI if necessary for Contractor's proper management and administration and to carry out its legal responsibilities; and,
  - 2) Disclose PHI and/or ePHI for the purpose of Contractor's proper management and administration or to carry out its legal responsibilities, only if:
    - a) The disclosure is required by law; or,
    - b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor will disclose such PHI and/or ePHI that the person will:
      - i. Hold such PHI and/or ePHI in confidence and use or further disclose it only for the purpose for which Contractor disclosed it to the person, or as required by law; and,
      - ii. Notify County of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,
  - 3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,
  - 4) De-identify all PHI and/or ePHI of County received by Contractor under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or Security Rule and does not preclude timely payment and/or claims processing and receipt.
- C. Notwithstanding the foregoing, in any instance where applicable state and/or federal laws and/or regulations are more stringent in their requirements than the provisions of HIPAA, including, but not limited to, prohibiting disclosure of mental health and/or substance abuse records, the applicable state and/or federal laws and/or regulations shall control the disclosure of records.

3. **Prohibited Uses and Disclosures.**

- A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.
- B. Contractor may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, or as required by law.
- C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.
- D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:
  - 1) Not to use or disclose PHI for fundraising , unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;
  - 2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);
  - 3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,
  - 4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Contractor for services provided pursuant to the Underlying Agreement.

4. **Obligations of County.**

- A. County agrees to make its best efforts to notify Contractor promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
- B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
- C. County agrees to make its best efforts to promptly notify Contractor in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Contractor's use or disclosure of PHI and/or ePHI.
- D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.
- E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

5. **Obligations of Contractor.** In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:
- A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e). Contractor shall also comply with the additional privacy requirements that are applicable to covered entities in HITECH, as may be amended from time to time.
  - B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum or as required by law. Contractor shall promptly notify County if Contractor is required by law to disclose PHI and/or ePHI.
  - C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum.
  - D. Mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by Contractor in violation of this Addendum.
  - E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410.
  - F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.
  - G. Make available to County or the Secretary, in the time and manner designated by County or Secretary, Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County, or created or received by Contractor on behalf of County, for purposes of determining, investigating or auditing Contractor's and/or County's compliance with the Privacy Rule.
  - H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).
  - I. Comply with requirements of satisfactory assurances under 45 CFR §164.512 relating to notice or qualified protective order in response to a third party's subpoena, discovery request, or other lawful process for the disclosure of PHI, which Contractor shall promptly notify County upon Contractor's receipt of such request from a third party.
  - J. Not require an individual to provide patient authorization for use or disclosure of PHI as a condition for treatment, payment, enrollment in any health plan (including the health plan administered by County), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by County.
  - K. Use appropriate administrative, technical and physical safeguards to prevent inappropriate use, disclosure, or access of PHI and/or ePHI.
  - L. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.
  - M. Comply with the requirements of the Privacy Rule that apply to the County to the extent Contractor is to carry out County's obligations under the Privacy Rule.
  - N. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.

6. **Access to PHI, Amendment and Disclosure Accounting.** Contractor agrees to:
- A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to County or an individual as directed by County, within five (5) days of request from County, to satisfy the requirements of 45 CFR §164.524.
  - B. **Amendment of PHI.** Make PHI available for amendment and incorporate amendments to PHI in a designated record set County directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from County, in accordance with 45 CFR §164.526.
  - C. **Accounting of disclosures of PHI and electronic health record.** Assist County to fulfill its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528 and, where applicable, electronic health records under 42 USC §17935(c) if Contractor uses or maintains electronic health records. Contractor shall:
    - 1) Document such disclosures of PHI and/or electronic health records, and information related to such disclosures, as would be required for County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record in accordance with 45 CFR §164.528.
    - 2) Within fifteen (15) days of receiving a written request from County, provide to County or any individual as directed by County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.
    - 3) Make available for County information required by this Section 6.C for six (6) years preceding the individual's request for accounting of disclosures of PHI, and for three (3) years preceding the individual's request for accounting of disclosures of electronic health record.
7. **Security of ePHI.** In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall:
- A. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;
  - B. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;
  - C. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
  - D. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;
  - E. Ensure compliance with the Security Rule by Contractor's workforce;
  - F. In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;
  - G. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,

H. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.

8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Contractor shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.

A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.

1) **Breaches treated as discovered.** A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).

2) **Content of notification.** The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Contractor:

a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;

b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

f) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

B. **Cooperation.** With respect to any breach of unsecured PHI reported by Contractor, Contractor shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.

C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Contractor shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.

D. **Delay of notification authorized by law enforcement.** If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.

- E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Contractor's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.
- F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.
- G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).
  - 1) Contractor agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.
  - 2) Contractor agrees to report to County any unlawful or unauthorized access, use, or disclosure of patient's medical information without unreasonable delay and no later than two (2) business days after Contractor detects such incident. Contractor further agrees such report shall be made in writing, and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unlawful or unauthorized access, use, or disclosure as defined above in this section, understanding and acknowledging that the term "breach" as used in Section 8.A.2 does not apply to California Health & Safety Code §1280.15.

9. **Hold Harmless/Indemnification.**

- A. Contractor agrees to indemnify and hold harmless County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Contractor, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Addendum, including but not limited to property damage, bodily injury, death, or any other element of any kind or nature whatsoever arising from the performance of Contractor, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. Contractor shall defend, at its sole expense, all costs and fees, including but not limited to attorney fees, cost of investigation, defense and settlements or awards, of County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents or representatives in any claim or action based upon such alleged acts or omissions.
- B. With respect to any action or claim subject to indemnification herein by Contractor, Contractor shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of County, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of County; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Contractor's indemnification to County as set forth herein. Contractor's obligation to defend, indemnify and hold harmless County shall be subject to County having given Contractor written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Contractor's expense, for the defense or settlement thereof. Contractor's



obligation hereunder shall be satisfied when Contractor has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.

- C. The specified insurance limits required in the Underlying Agreement of this Addendum shall in no way limit or circumscribe Contractor's obligations to indemnify and hold harmless County herein from third party claims arising from issues of this Addendum.
- D. In the event there is conflict between this clause and California Civil Code §2782, this clause shall be interpreted to comply with Civil Code §2782. Such interpretation shall not relieve the Contractor from indemnifying County to the fullest extent allowed by law.
- E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Addendum, this indemnification shall only apply to the subject issues included within this Addendum.

10. **Term.** This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Contractor, or created or received by Contractor on behalf of County, is destroyed or returned to County, or, if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.

11. **Termination.**

A. **Termination for Breach of Contract.** A breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement with or without an opportunity to cure the breach, notwithstanding any provision in the Underlying Agreement to the contrary. Either party, upon written notice to the other party describing the breach, may take any of the following actions:

- 1) Terminate the Underlying Agreement and this Addendum, effective immediately, if the other party breaches a material provision of this Addendum.
- 2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party in a timely manner, the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.
- 3) If termination of the Underlying Agreement is not feasible, the breaching party, upon the request of the non-breaching party, shall implement, at its own expense, a plan to cure the breach and report regularly on its compliance with such plan to the non-breaching party.

B. **Effect of Termination.**

- 1) Upon termination of this Addendum, for any reason, Contractor shall return or, if agreed to in writing by County, destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.
- 2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Contractor maintains such PHI and/or ePHI.

12. **General Provisions.**

- A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation for 6 years from the date of its creation or as otherwise prescribed by law, whichever is later.
- B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.
- C. **Survival.** The obligations of Contractor under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.
- D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.
- E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.
- F. **Interpretation of Addendum.**
  - 1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.
  - 2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.
- G. **Notices to County.** All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer: HIPAA Privacy Manager

County HIPAA Privacy Officer Address: 26520 Cactus Avenue,  
Moreno Valley, CA 92555

County HIPAA Privacy Officer Phone Number: (951) 486-6471










# Securance Risk Assessment Agreement - Final 0818

Final Audit Report

2023-08-18

Created:	2023-08-18
By:	israel gomez (israel.gomez1987@gmail.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAHKVH9sswTFkkonsPYNjeelPtuGIWUzC6

## "Securance Risk Assessment Agreement - Final 0818" History

-  Document created by israel gomez (israel.gomez1987@gmail.com)  
2023-08-18 - 10:45:58 PM GMT
-  Document emailed to Paul Ashe (pashe@securanceconsulting.com) for signature  
2023-08-18 - 10:46:13 PM GMT
-  Email viewed by Paul Ashe (pashe@securanceconsulting.com)  
2023-08-18 - 11:12:30 PM GMT
-  Document e-signed by Paul Ashe (pashe@securanceconsulting.com)  
Signature Date: 2023-08-18 - 11:13:32 PM GMT - Time Source: server
-  Document emailed to Tawn Lieu (tlieu@rivco.org) for signature  
2023-08-18 - 11:13:35 PM GMT
-  Email viewed by Tawn Lieu (tlieu@rivco.org)  
2023-08-18 - 11:15:36 PM GMT
-  Signer Tawn Lieu (tlieu@rivco.org) entered name at signing as Tawny Lieu  
2023-08-18 - 11:36:14 PM GMT
-  Document e-signed by Tawny Lieu (tlieu@rivco.org)  
Signature Date: 2023-08-18 - 11:36:16 PM GMT - Time Source: server
-  Agreement completed.  
2023-08-18 - 11:36:16 PM GMT