MODIFICATION NUMBER ONE OF AGREEMENT FOR SERVICES BETWEEN COUNTY OF SONOMA AND SECURANCE LLC

On June 1, 2023, the County of Sonoma, a political subdivision of the State of California, (hereinafter "County") and Securance LLC (hereinafter "Contractor") entered into a services agreement (hereinafter "Agreement").

Pursuant to Section 13.7 (Merger) of the Agreement, the parties hereby evidence their intent and desire to modify the Agreement as follows:

1. Exhibit A (Scope of Work and Budget) is hereby deleted and replaced in its entirety with the attached Exhibit A (Scope of Work and Budget).
2. Exhibit B (Insurance Requirements) is hereby deleted and replaced in its entirety with the attached Exhibit B (Insurance Requirements).
3. Section 2.1 (Payment for Services) is hereby revised to read as follows:

2.1. Payment for Services

For all services and incidental costs required hereunder, Contractor shall be paid multiple lump sum amounts as listed below, regardless of the number of hours or length of time necessary for Contractor to complete the services. Contractor shall not be entitled to any additional payment for any expenses incurred in completion of the services. A breakdown of costs used to derive the lump sum amount, including but not limited to hourly rates, estimated travel expenses and other applicable rates, is specified in Exhibit A (Scope of Work and Budget).

Milestone Description	CY 2023* Amount ($)	CY 2024 Amount ($)	CY 2025 Amount ($)	CY 2026 Amount ($)	CY 2027 Amount ($)	Total ($)
Completion of Kickoff Meeting (10%)	5,580.00	5,803.20	6,945.30	7,500.90	8,101.00	33,930.40
Completion of Assessment Work (70%)	39,060.00	40,622.40	48,617.10	52,506.30	56,707.00	237,512.80
Delivery of Final Report (20%)	11,160.00	11,606.40	13,890.60	15,001.80	16,202.00	67,860.80
Totals ($)	**55,800.00**	**58,032.00**	**69,453.00**	**75,009.00**	**81,010.00**	**339,304.00**

*Calendar Year (CY) 2023 period begins May 1, 2023 and ends December 31, 2027.

Upon completion of the work, Contractor shall submit its bill[s] for payment in a form approved by County's Auditor and the Head of the County Department receiving the services. The bill[s] shall identify the services completed and the amount charged. Expenses not expressly authorized by the Agreement shall not be reimbursed.

Unless otherwise noted in this agreement, payments shall be made within the normal course of County business after presentation of an invoice in a form approved by County for services performed. Payments shall be made only upon the satisfactory completion of the services as determined by County.

4. Section 2.2 (Maximum Payment Obligation) is hereby revised to read as follows:

   2.2. Maximum Payment Obligation

   In no event shall County be obligated to pay Contractor more than the total sum of $339,304, including $55,800 for Calendar Year (CY) 2023 (beginning May 1, 2023), $58,032 for CY 2024, $69,453 for CY 2025, $75,009 for CY 2026, and $81,010 for CY 2027 under the terms and conditions of this Agreement.

5. Article 3 (Term of Agreement) is hereby revised to read as follows:

   3. Term of Agreement

   The term of this Agreement shall be from May 1, 2023 to December 31, 2027, unless terminated earlier in accordance with the provisions of Article 4 (Termination).

6. Article 12 (Method and Place of Giving Notice, Submitting Bills, and Making Payments) is hereby revised to read as follows:

   12. Method and Place of Giving Notice, Submitting Bills, and Making Payments

   All notices, bills, and payments shall be made in writing and shall be given by personal delivery or by U.S. mail or courier service. Notices, bills, and payments shall be addressed as follows:

To County	To Contractor
Ken Tasseff Healthcare Privacy & Security Officer Department of Health Services County of Sonoma 1450 Neotomas Avenue, Suite 200 Santa Rosa CA 95405 707-565-4703 Ken.Tasseff@sonoma-county.org	Shawn Marsh Governmental Contract and Proposal Manager Securance LLC 13916 Monroes Business Park, Suite 102 Tampa Florida 33635 877-578-0215 smarsh@securanceconsulting.com

   When a notice, bill, or payment is given by a generally recognized overnight courier service, the notice, bill, or payment shall be deemed received on the next business day. When a copy of a notice, bill, or payment is sent by facsimile or email, the notice, bill, or payment shall be deemed received upon transmission as long as: (1) the original copy of the notice, bill, or payment is promptly deposited in the U.S. mail and postmarked on the date of the facsimile or email (for a payment, on or before the due date); (2) the sender has a written confirmation of the facsimile transmission or email; and (3) the facsimile or email is transmitted before 5 p.m. (recipient's time). In all other instances, notices, bills, and payments shall be effective upon receipt by the recipient. Changes may be made in the names and addresses of the person to whom notices are to be given by giving notice pursuant to this Article 12.

Except as expressly modified herein, all terms and conditions of Agreement shall remain in full force and effect.

§ The remainder of this page has intentionally been left blank. §

IN WITNESS WHEREOF, the parties have caused this modification to be duly executed by their authorized representatives this __________ day of ______________________, 2024.

CONTRACTOR:

[redacted]

9-20-2024

Paul Ashe, President
Securance LLC

Dated

COUNTY OF SONOMA:
Approved; Certificates of Insurance on File with County:

~~Tina Rivera, Director~~ Jennifer Solito, Interim Director
Department of Health Services

Dated

Approved as to Substance:

[redacted]

09/27/24

Division Director or Designee

Dated

Approved as to Form:

[redacted]

9-19-24

Sonoma County Counsel

Dated

Approved as to Substance:

[redacted] signed on behalf of Ken Tasseff

09/11/2024

Privacy & Security Officer or Designee

Dated

Exhibit A. Scope of Work and Budget

STATEMENT OF REQUIREMENTS

The Contractor shall perform the categories of services identified in sections 1. through 5. below. All sections referenced below are from Title 45 of the CFR.

1. HIPAA Risk Analysis (45 CFR §164.308(a)(1)(ii)(A))

The HIPAA Risk Analysis must be conducted in accordance with the National Institute of Standards and Technology (NIST), International Standards Organization (ISO).

Proposer shall perform the following:

a. Penetration Testing (i.e., blind, and intelligent)
b. Vulnerability Assessment
c. Physical assessment of technical infrastructure
d. A systematic and thorough identification and evaluation of the County's information assets (data, information systems, and information processing facilities) which create, receive, maintain, or transmit electronic ePHI
e. Potential risks to those identified information assets (to include potential costs of privacy or security breaches and other information security threats), and associated with how the department collects, uses, manages, stores, maintains, discloses, and disposes of information
f. Existing privacy and security measures and the effectiveness of those measures
g. Potential gaps or deficiencies in maintenance, protection, and utilization of the information assets
h. Internal/external networks (including penetration tests)
i. Internet/intranet vulnerability test
j. Internet, Extranet, and Intranet applications
k. Wireless networks, including, but not limited to, secure and guest Wi-Fi access points.
l. Servers and data storage.
m. Workstations and peripheral endpoints
n. Firewall diagnostics
o. Virtual Private Network and remote access infrastructure
p. Mobile devices
q. Denial of service tests
r. Social engineering tests
s. Network architecture review
t. Other items identified by the Proposer as recommended or necessary for a Risk Analysis

2. HIPAA Security Rule Gap Analysis – Addresses compliance with:

a. §164.306 General Requirements
b. §164.308 Administrative Safeguards
c. §164.310 Physical Safeguards
d. §164.312 Technical Safeguards
e. §164.316 Policies, Procedures and Documentation

3. Privacy Rule Gap Analysis – Addresses compliance with:

a. §164.502: Uses and Disclosure of Protected Health Information: General Rules
b. §164.504: Uses and Disclosures: Organizational Requirements
c. §164.506: Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations

d. §164.508: Uses and Disclosures for Which an Authorization is Required
e. §164.510: Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object
f. §164.512: Uses and Disclosures for Which an Authorization or Opportunity to agree or Object is Not Required
g. §164.514: Other Requirements Relating to Uses and Disclosures of Protected Health Information.
h. §164.520: Notice of Privacy Practices for Protected Health Information
i. §164.522: Rights to Request Privacy Protection for Protected Health Information
j. §164.524: Access of Individuals to Protected Health Information
k. §164.526: Amendment of Protected Health Information
l. §164.528: Accounting of Disclosures of Protected Health Information
m. §164.530: Administrative Requirements

4. HIPAA PHYSICAL ASSESSMENT AND END USER SECURITY AWARENESS ASSESSMENT

a. Site visits as determined by the participating department to evaluate and document physical security controls that are currently implemented.
b. Other activities identified by Proposer as recommended or necessary for a physical assessment.
c. End User Security Awareness Assessment

   i. Interviews with selected staff regarding common privacy and security related practices within and between departments to measure end user security awareness.

   ii. A review of existing privacy and security policies and procedures at both the department and County level, including policies regarding: breach reporting and response; personnel; business associate agreements; physical, technical and administrative safeguards; oversight and monitoring; and HIPAA complaints.

   iii. A review and evaluation of department and County level HIPAA training.

   iv. Other activities identified by Proposer as recommended or necessary for assessing end user security awareness.

5. SERVICE REQUIREMENTS

a. The capacity to initiate contact with departments within 15 days of Contract approval. The selected proposer must work with the individual department to identify the scope of the assessment for that specific department, project schedule, dates of availability, and other issues as needed.
b. Participation on a County workgroup(s) utilized and conducted to manage the awarded contract, tentatively expected to meet on a monthly basis.
c. Regular reports during the assessment period must be provided to the participating departments. Proposers are requested to propose a plan for keeping departments informed and up to date on progress and issues as they arise.
d. At the conclusion of each assessment, documentation must be provided that fulfills the HIPAA/HITECH risk assessment requirements and provides an admissible report for state and federal audits.
e. The results of each assessment must be detailed in a report which at a minimum addresses the following:

   i. A review of the current state of the department.

   ii. A list of deficiencies for the department, in report and data formats. All deficiencies must be tied to a HIPAA Rule and location as well as a system, process, etc., so remediation can be focused.

iii. The threats and vulnerabilities to the County's information, including probability and impact of each threat and vulnerability, using industry standards and best practices.

iv. Detailed recommended remediation measures for each identified threat, vulnerability, and deficiency. Work with the CE departments involved with the remediation and include the estimated costs for each recommendation.

v. For "addressable" HIPAA specifications that are determined to be unreasonable or inappropriate, document alternative security measures that are being implemented and how the alternative measures meet the standard. If not applicable, document the reason why the HIPAA implementation specification is not reasonable and appropriate and how the higher-level standard is being met.

vi. Work with the Privacy Officer and the departments involved with the remediation to create a milestone-based work plan with a timeline for the CE department to implement the recommended remediation measures.

f. The final report shall be directed to:
Tashawn Sanders, Chief Deputy County Counsel Office of County Counsel,
575 Administration Drive, #105A Santa Rosa, CA. 95403

g. In addition to the detailed report, an executive summary report must be prepared summarizing the scope, approach, findings, and recommendations in a manner suitable for senior management. At the discretion of the department, a formal on-site final presentation to the department's senior management of the findings and recommendations may be requested.
h. During the assessment period, departments may request meetings to proactively manage risks and issues which might impact the quality of the assessment.
i. The Proposal must address the method with which the Proposer will prioritize the assessment of the departments, and the amount of staffing available to ensure all departments are assessed within the contract period.
j. The confidentiality of the analysis and final reports must be maintained at all times. Proposers must discuss how confidentiality is maintained during the analysis process.
k. It is expected that project staff will remain consistent during the Contract period unless prior authorization is received from the County.
l. Proposers must supply their own hardware, software, media, and materials required to complete the awarded contract.

6. Organizational Considerations

As stated in Section A(1) above, the County has five (5) covered components to the Covered Entity. They are:

a. Department of Health Services – Public Health, Behavioral Health and Administration, and add Homelessness Services to scope for 2025, 2026, and 2027 Security Risk Assessments.
b. County Counsel (Approximately 5 staff)
c. Human Resources – Self-Funded Health Plan, FSA, Liability, and Insurance Unit
d. Information Services Department
e. Human Services Department - Multipurpose Senior Services Program and Home Community Based Alternatives Program. (Approximately 5 staff in each program)

7. ADDITIONAL NOTES

The first four covered components (a. through d.) use the same IT system and architecture, managed by the County's Information Services Department. The Department of Health Services is the largest covered component with approximately 600 HIPAA regulated staff and four electronic medical record systems. Human Resources has approximately 8 staff managing a self-funded health plan, a flexible spending account, and a liability and insurance unit, all subject to HIPAA. County Counsel is an internal business associate that includes approximately 5 staff exposed to PHI.

The fifth covered component (e.), Human Services Department (HSD) has a separate and distinct IT system and architecture. While HSD has approximately 800 staff, the covered component portion of the department, (Multipurpose Senior Services Program and Home Community Based Alternatives Program.) is limited to approximately 12 staff. Client records are stored on a California State data system and is entered via secure portal.

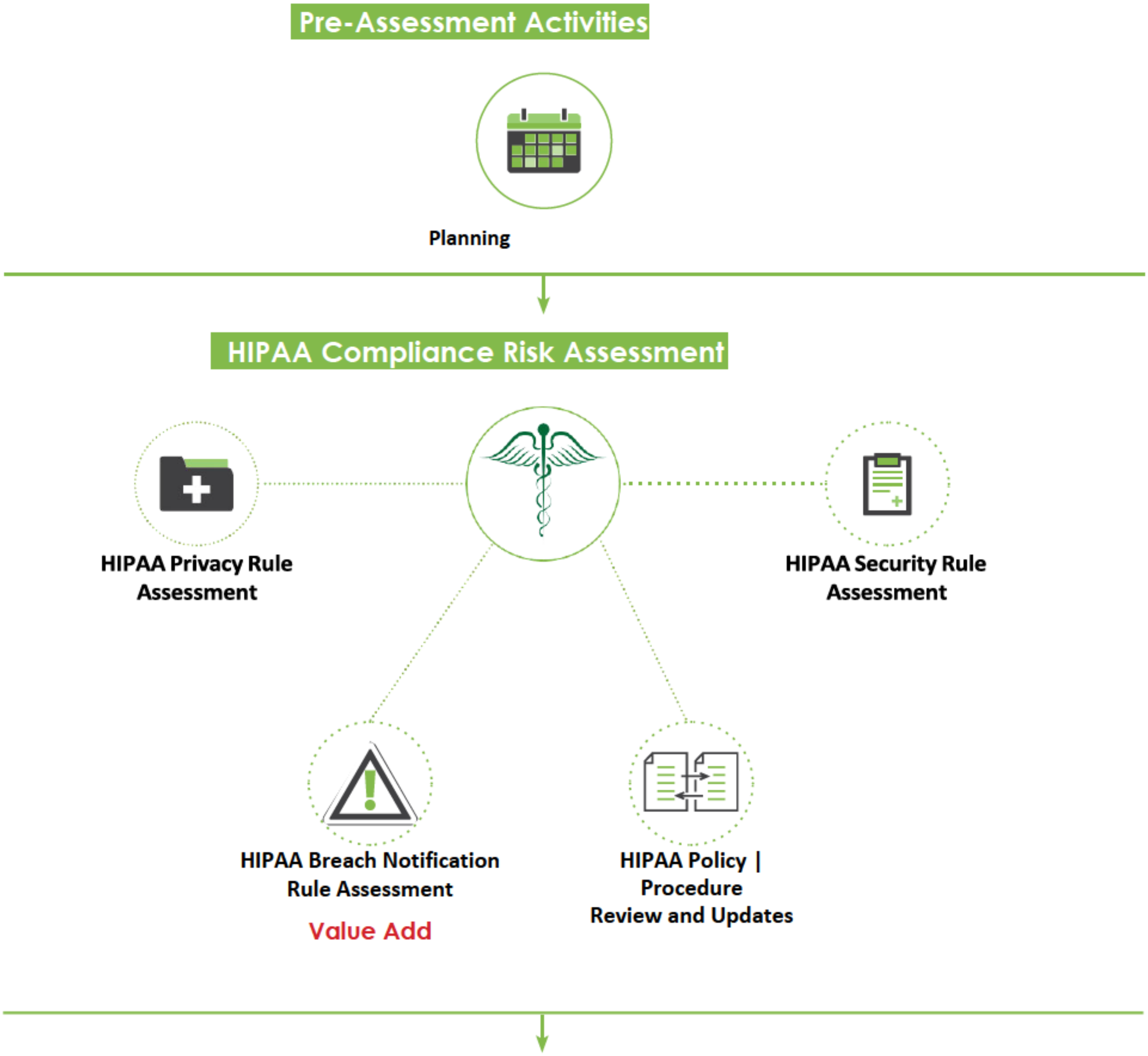
Proposers should be aware that this RFP includes the assessment of two separate and distinct IT systems with some commonalities.

Work Plan — Proposed Scope

a. Preliminary detailed work plan to include process and methodologies for the scope of work desired for this project.

Proposed Scope

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



Pre-Assessment Activities

Planning

HIPAA Compliance Risk Assessment

HIPAA Privacy Rule Assessment

HIPAA Security Rule Assessment

HIPAA Breach Notification Rule Assessment

Value Add

HIPAA Policy | Procedure Review and Updates

Work Plan — Proposed Scope (continued)

Technical Testing

- External Network Vulnerability Assessment and Penetration Test
  Value Add
- Web Application Testing
- Firewall Configuration Review
- Internal Network Vulnerability Assessment and Penetration Testing
- Wireless Network Assessment
- Enterprise Application Testing
- Endpoint Configuration Review
- Server Configuration | Operating System Review
- Physical Security Assessment
- Mobile Device Security Assessment
- Virtual Private Network (VPN) Review
- Network Architecture Review
- Social Engineering: Phishing
  Value Add

Deliverables

- Reporting

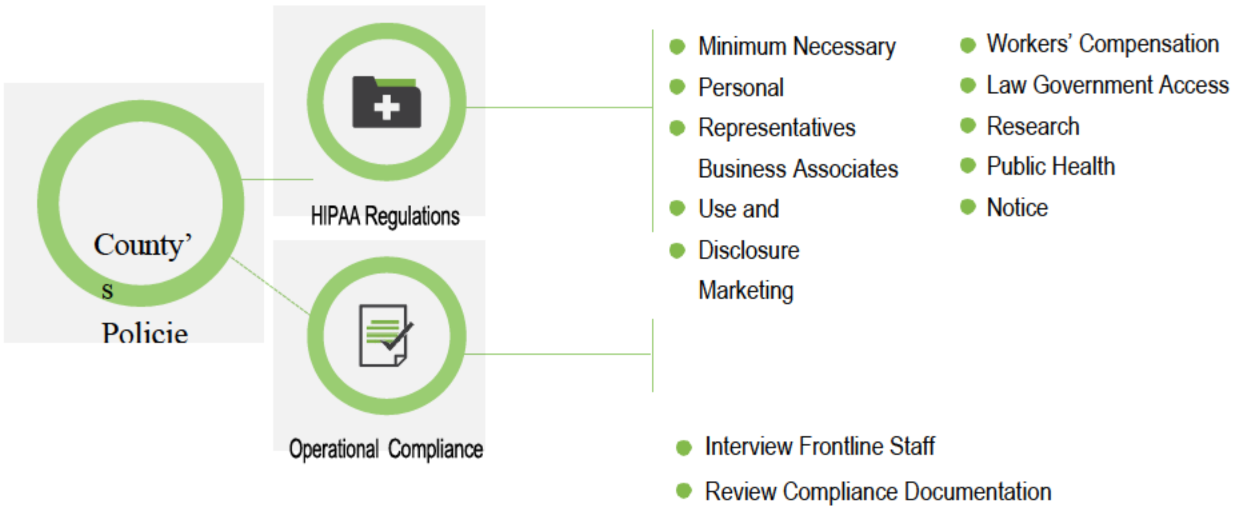
Section III — Project Approach and Work Schedule

Work Plan — HIPAA Privacy Rule Compliance Assessment

Privacy Rule

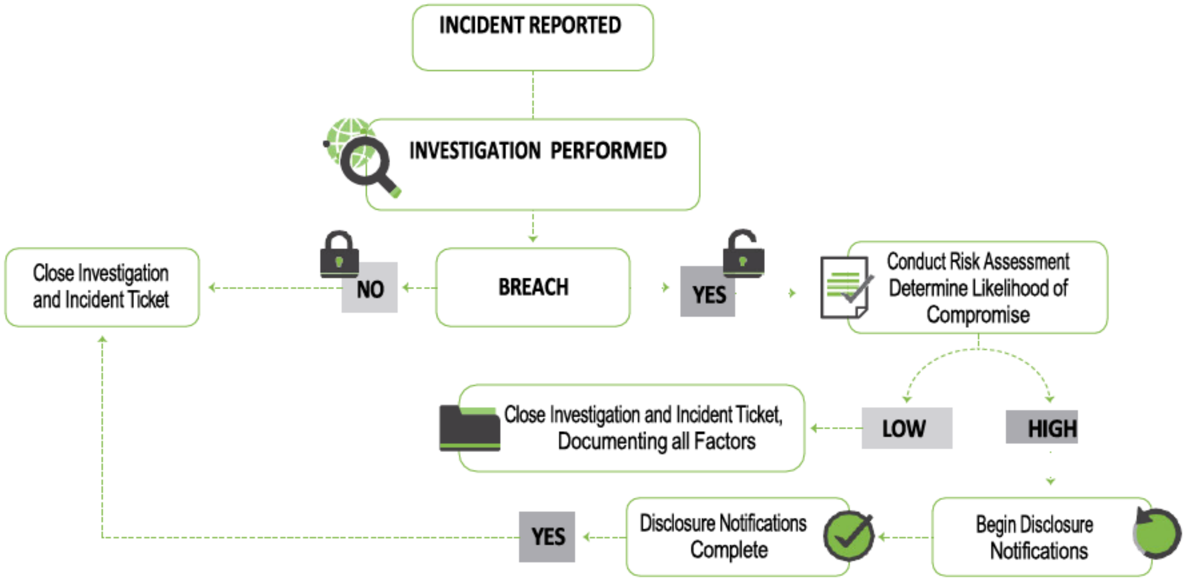
Our HIPAA Privacy Rule compliance assessment is a comprehensive analysis of an organization's adherence to all applicable Sections of the Rule, per §45 Code of Federal Regulations (CFR). Our proven approach involves mapping your policies to the Rule's Sections, assessing your level of compliance following 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.


INCIDENT REPORTED
INVESTIGATION PERFORMED
BREACH
NO
Close Investigation and Incident Ticket
YES
Conduct Risk Assessment Determine Likelihood of Compromise
LOW
HIGH
Close Investigation and Incident Ticket, Documenting all Factors
Begin Disclosure Notifications
Disclosure Notifications Complete
YES

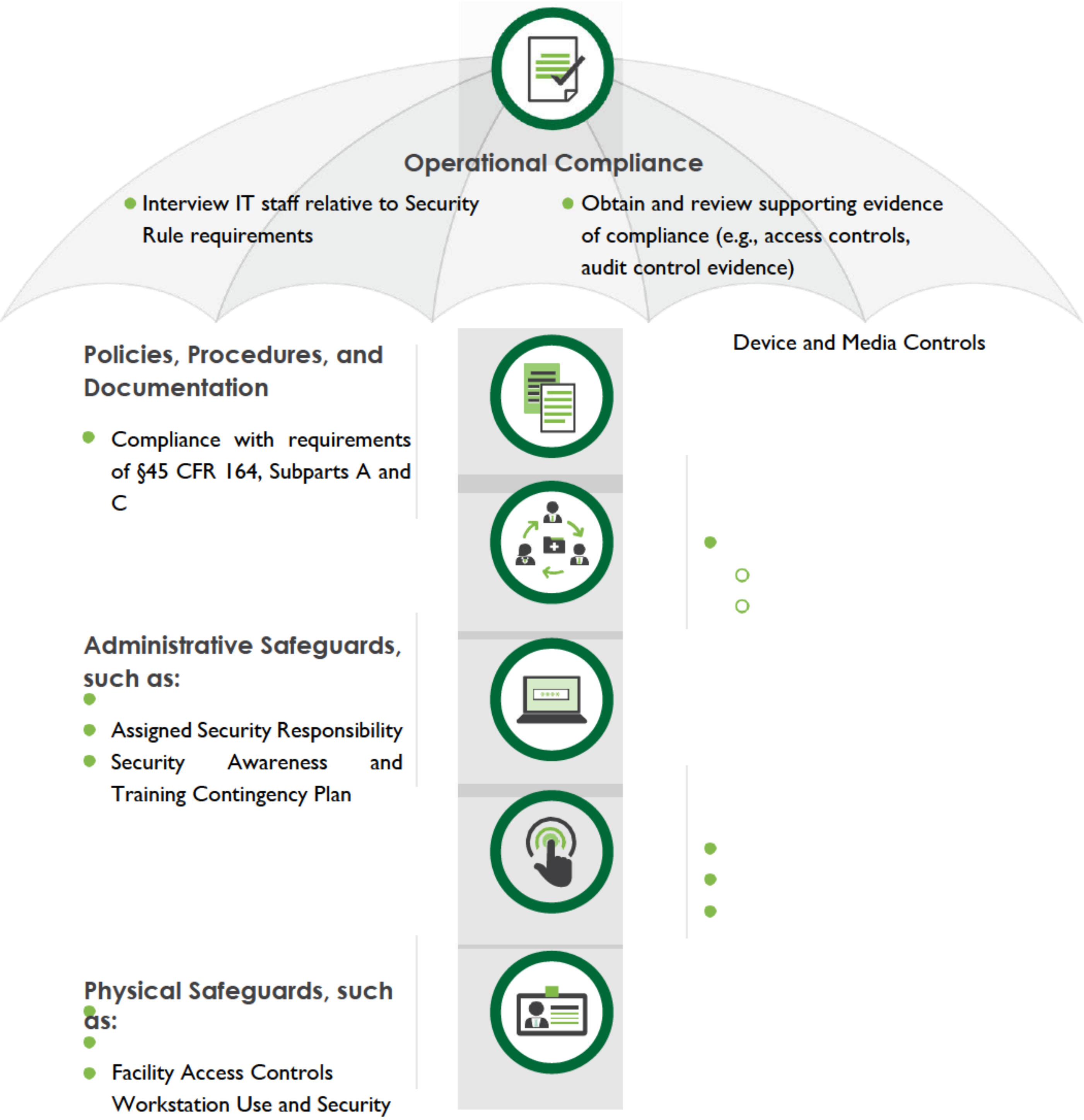
Section III — Project Approach and Work Schedule

Work Plan — HIPAA Privacy Rule Compliance Assessment

(continued) Security Rule

The Securance HIPAA Security Rule compliance assessment methodology includes a comprehensive analysis of the organization's adherence to all applicable Sections of the Rule, per §45 CFR. Our proven approach involves mapping your environment to the Security Rule's Sections and assessing your level of compliance following the OCR audit protocol.

We will ensure County's IT policies are mapped to the Security Rule and review:



Operational Compliance

- Interview IT staff relative to Security Rule requirements
- Obtain and review supporting evidence of compliance (e.g., access controls, audit control evidence)

Policies, Procedures, and Documentation

- Compliance with requirements of §45 CFR 164, Subparts A and C

Device and Media Controls

Administrative Safeguards, such as:

- Assigned Security Responsibility
- Security Awareness and Training Contingency Plan

Physical Safeguards, such as:

- Facility Access Controls

Workstation Use and Security

Section III — Project Approach and Work Schedule

Organizational Requirements

Compliance with:

Business Associate

Contracts

Group Health Plans

Technical Safeguards, such as:

Access Control

Information Integrity

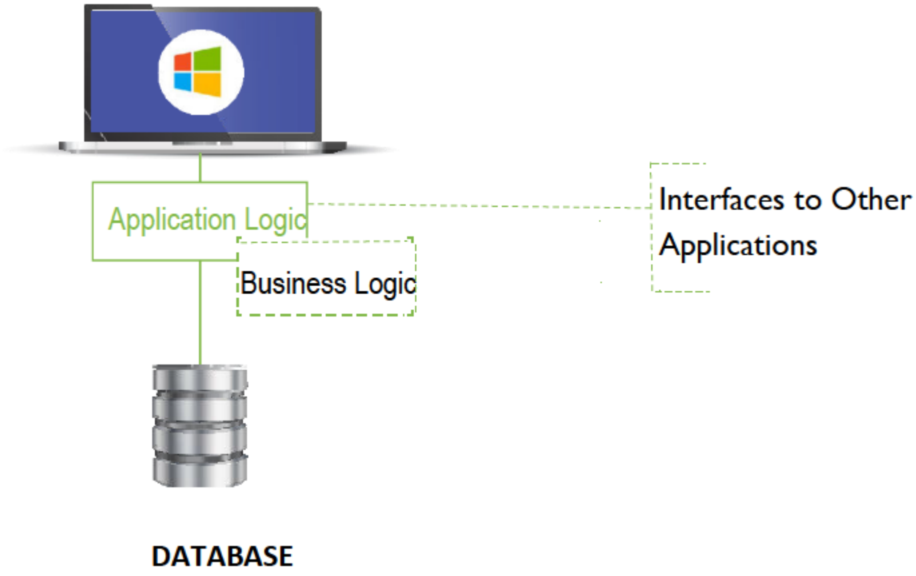
Transmission Security

Section III — Project Approach and Work Schedule

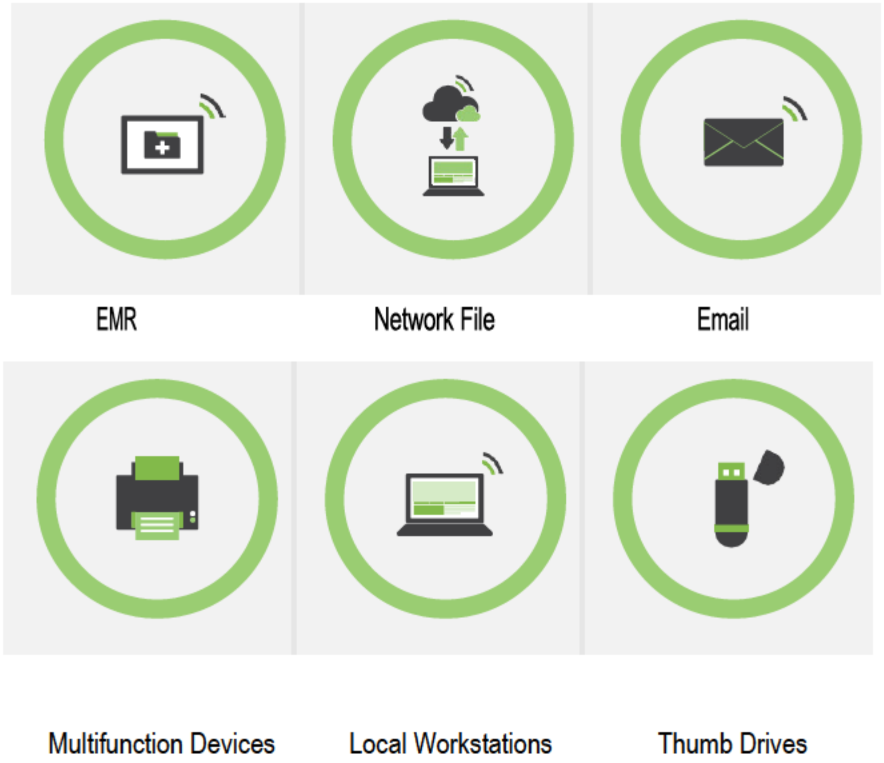
Work Plan — HIPAA Privacy Rule Compliance Assessment (continued)

ePHI Information Assets

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



Securance identifies all areas where ePHI can live, including:

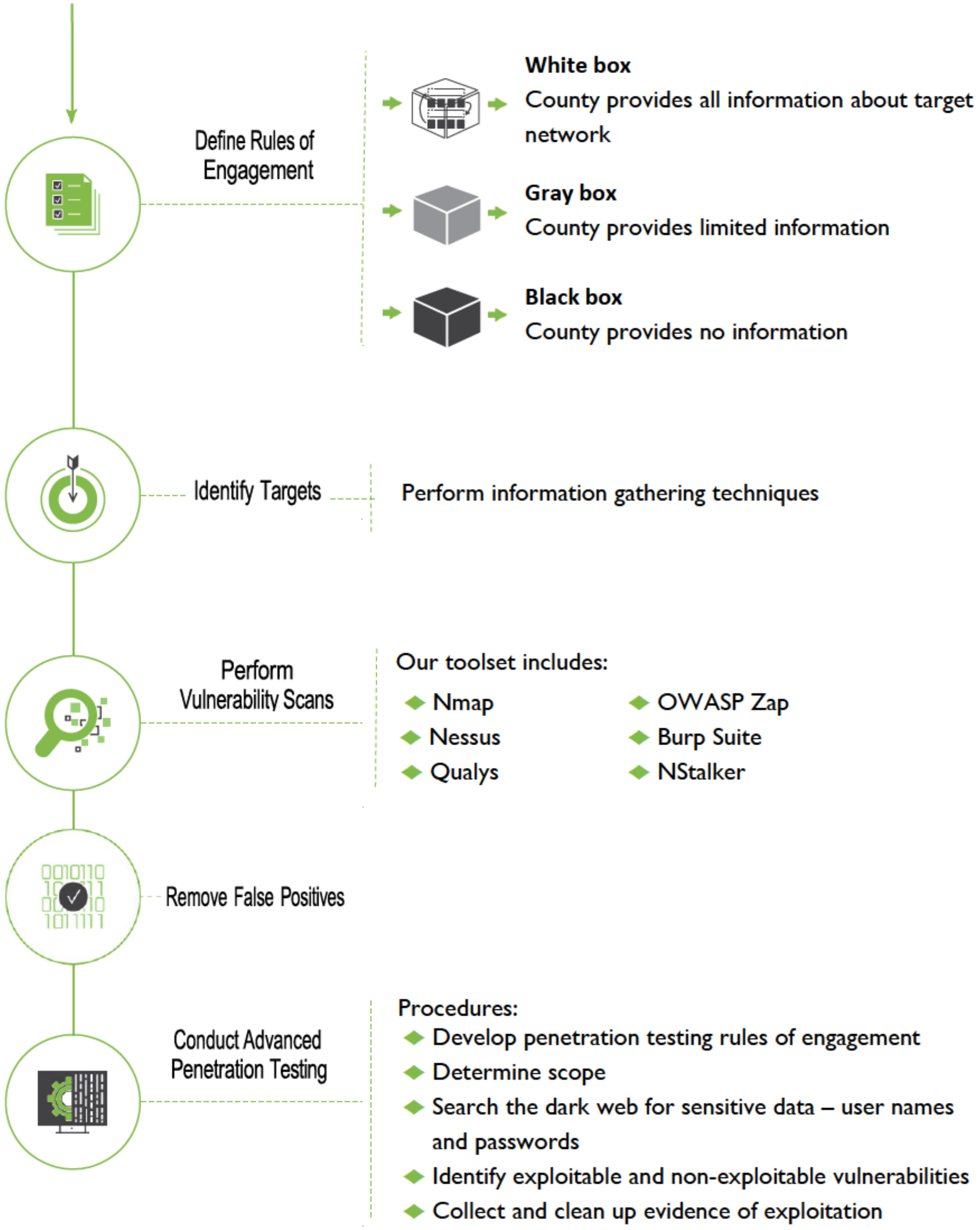


Section III — Project Approach and Work Schedule

Work Plan — External | Internal Vulnerability Assessment and 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



Define Rules of Engagement

White box
County provides all information about target network

Gray box
County provides limited information

Black box
County provides no information

Identify Targets

Perform information gathering techniques

Perform Vulnerability Scans

Our toolset includes:

- Nmap
- Nessus
- Qualys
- OWASP Zap
- Burp Suite
- NStalker

Remove False Positives

Conduct Advanced Penetration Testing

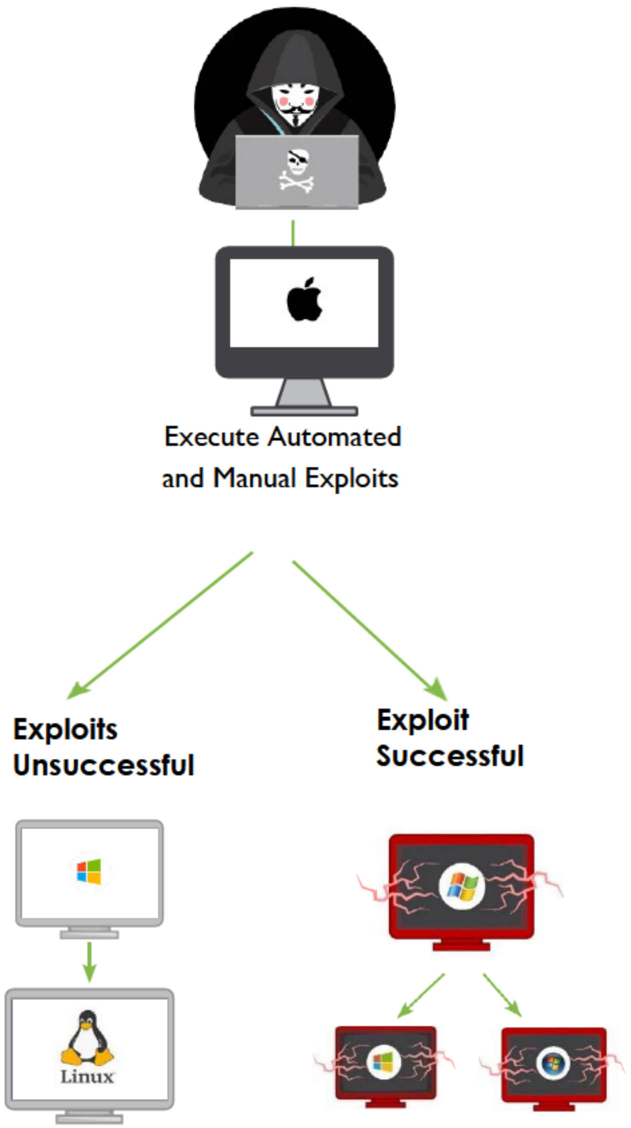
Procedures:

- Develop penetration testing rules of engagement
- Determine scope
- Search the dark web for sensitive data – user names and passwords
- Identify exploitable and non-exploitable vulnerabilities
- Collect and clean up evidence of exploitation

Section III — Project Approach and Work Schedule

Work Plan — External | Internal Vulnerability Assessment and Penetration Test (continued)

Securance's Ethical Penetration Testing Process



Execute Automated and Manual Exploits

Exploits Unsuccessful

Exploit Successful

Our toolset includes, but may not be limited to:

- Metasploit
- Core Impact
- Canvas
- Manual exploits (including dark web searches)

Email: Wendy.Hudson@sonoma-county.org

Hashed Password: 1788#$%RTTTerucnmD23@#$

Sourced from dark web

Other tools will be used, as required, to perform specific tasks.

To successfully exploit vulnerabilities, we will:

- Move laterally in the environment
- Escalate account privileges
- Attempt to exfiltrate data
- Leave trophy
- Clean up the environment

Section III — Project Approach and Work Schedule

Work Plan — Web Application Testing

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 I 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

Work Plan — Web Application Testing

Manual Testing

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

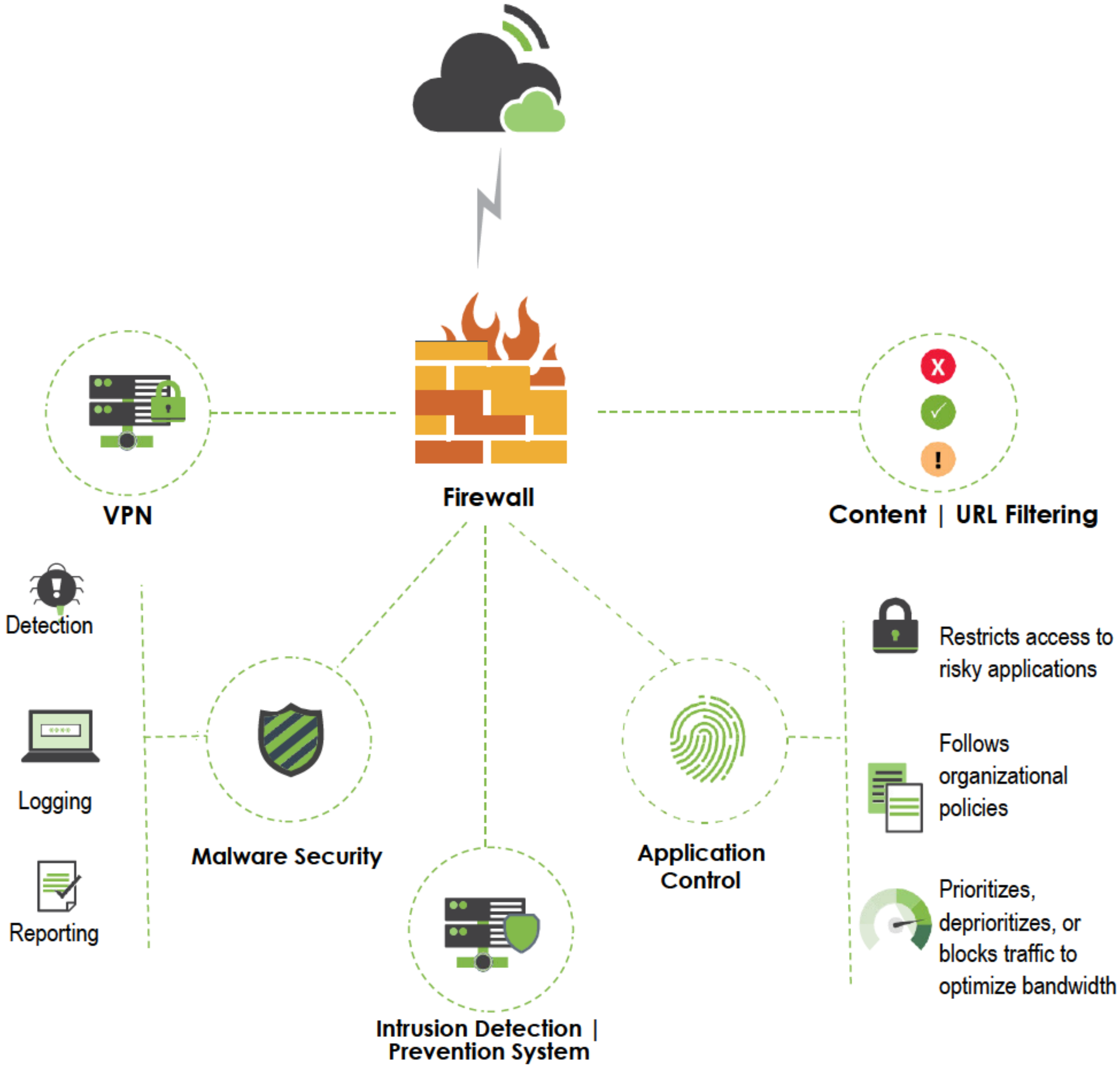
- URL manipulation
- Input field character testing
- Input field string sanitization testing
- Remote site return validation
- Software version vulnerability testing

Section III — Project Approach and Work Schedule

Work Plan — Firewall Configuration Review

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.


Firewall
VPN
Content | URL Filtering
Detection
Logging
Reporting
Malware Security
Intrusion Detection | Prevention System
Application Control
Restricts access to risky applications
Follows organizational policies
Prioritizes, deprioritizes, or blocks traffic to optimize bandwidth

Work Plan — Firewall Configuration Review (continued)

We will ensure:

All modules are dynamically configured to update in real time

Zone protection profiles are configured and consistent with internal network zones and VLANs

SSL (secure sockets layer) decryption is enabled and properly configured

Anti-malware definitions are updated in real time

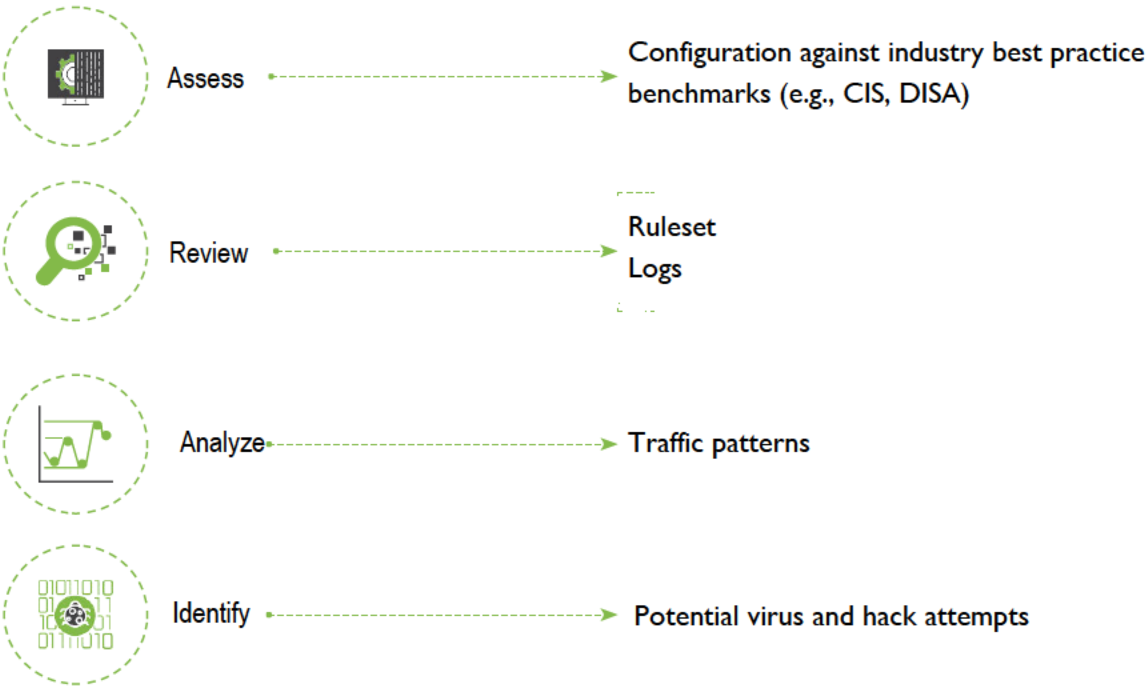
Vulnerability protection is enabled and validated against the most recent vulnerability database

URL filtering is enabled and up to date

File blocking is definition based

Data filtering is consistent with County's data classification standards

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



Assess → Configuration against industry best practice benchmarks (e.g., CIS, DISA)

Review → Ruleset
Logs

Analyze → Traffic patterns

Identify → Potential virus and hack attempts

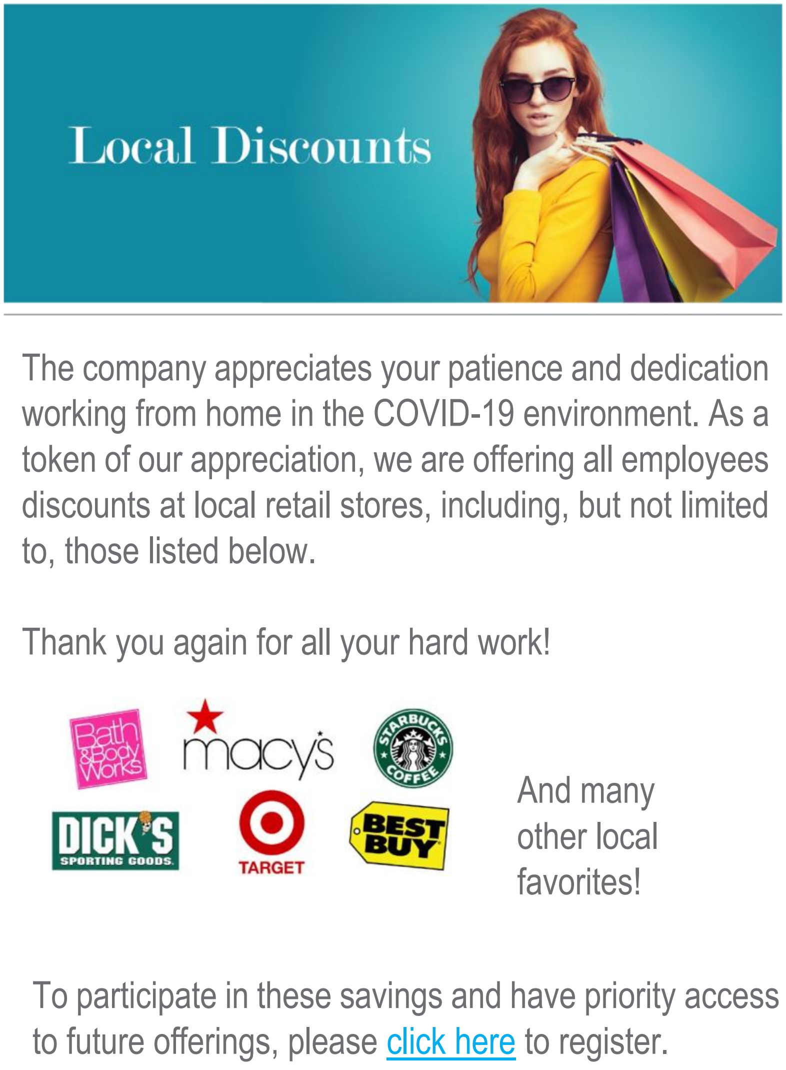
Section III — Project Approach and Work Schedule

Work Plan — Social Engineering

Securance performs all methods of social engineering testing, including email phishing

Our methodology:

- Ensures there are effective controls over the human element of security
- Verifies the security of organizational resources and sensitive information
- Identifies weakness in user security awareness programs



Local Discounts

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!

Bath & Body Works
macy's
Starbucks Coffee
Dick's Sporting Goods
Target
Best Buy

And many other local favorites!

To participate in these savings and have priority access to future offerings, please click here to register.

Securance's best practices white paper:

Unscammable: The Guide to Fostering a Culture of Security Awareness

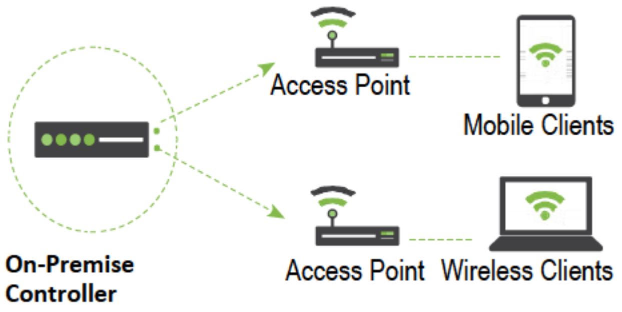
Scan the code with your smartphone or tablet camera to read the white paper

Section III — Project Approach and Work Schedule

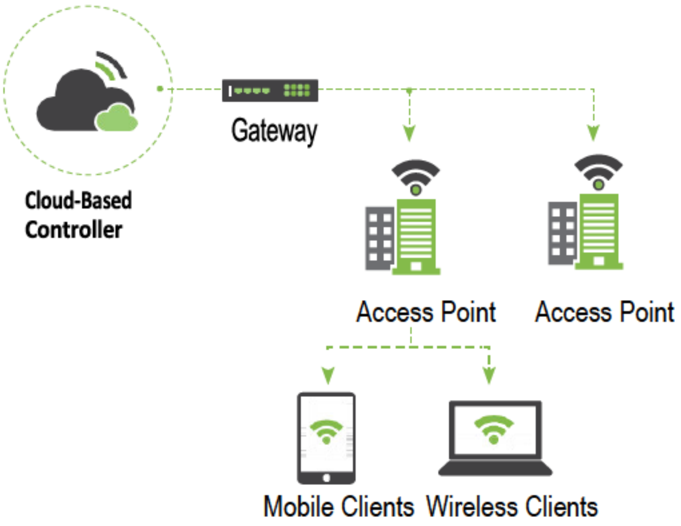
Work Plan — Wireless Network Assessment

Securance assesses the configuration and security of both controller and access point-based wireless networks.

Controller-Based Wireless Networks



- Assess controller configurations
- Evaluate rogue access point detection and management
- Uncover or identify hidden SSIDs
- Assess encryption strength
- Review network segmentation
- Review administrative access controls and logging
- Confirm access points can only receive configurations from the controller



We will evaluate cloud-based WiFi networks to the extent allowed by the cloud provider for the controls listed above.

Section III — Project Approach and Work Schedule

Work Plan — Wireless Network Assessment (continued)

Penetration Testing

Using assorted wireless radio devices, including Pineapple tools and various wireless adapters, we will intercept encrypted and unencrypted network packets.

Depending on the rules of engagement, we will:

Passively sniff and attempt to capture handshakes between the access point and client

Attempt to de-authenticate clients from the wireless network and capture the reestablished handshakes between the access point and client

Establish a rogue access point to lure client devices and capture their wireless authentication credentials

Attempt to crack the encrypted credentials and use them to breach the wireless network

After gaining access to the wireless network, we will:

- Deploy executables and scripts to gain a presence on the network
- Capture device and network information
- Escalate privileges
- Disable local firewalls and antivirus software
- Create a new privileged user
- Move laterally on the network to access and gain control of the domain controller(s)
- Exfiltrate data from host machines
- Hide evidence of our breach

Potential Tools Used

Vistumbler	Ncrack	Mimikatz
iStumbler	Hashcat	Wireshark
Kismet	John the Ripper	Advanced IP Scanner
Aircrack-ng suite	Online rainbow tables	
Besside-ng	Cain and Abel	

Section III — Project Approach and Work Schedule

Work Plan — Enterprise Application 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

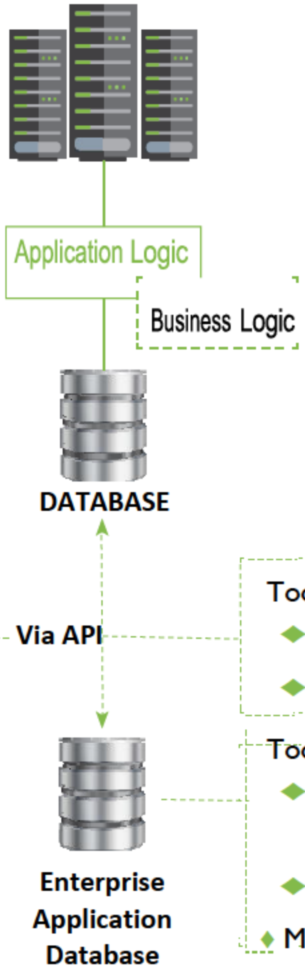
Securance will review configurable application control and tolerance settings. In addition, we will ensure that high-risk functions are restricted to authorized users and reviewed by management.

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.

Our API assessment includes:

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



Tools used:

- OWASP ZAP
- Burp Suite

Tools used:

- Application Detective
- Nessus Pro
- Manual procedures

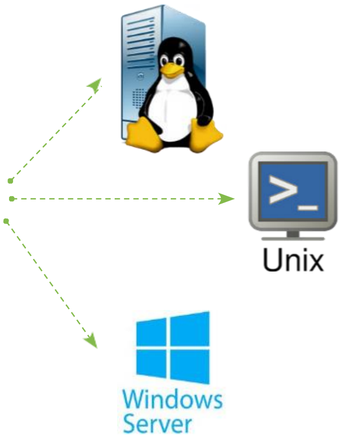
Work Plan — Enterprise Application Testing (continued)

Section III — Project Approach and Work Schedule

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 industry standards and best practices



IT General Controls

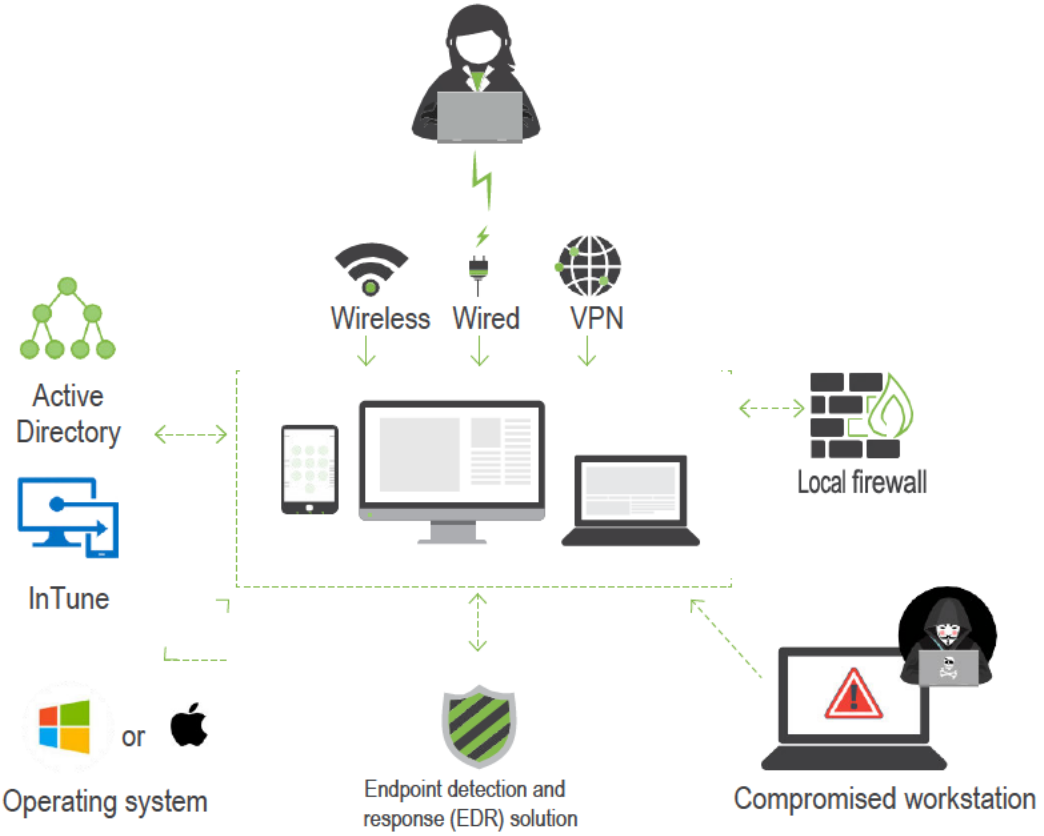
We will assess the IT general controls supporting the application environment and compare them to the NIST 800-53 framework.

- User provisioning
- System and data backup
- Disaster recovery
- Change management
- Patch management
- Data classification

Section III — Project Approach and Work Schedule

Work Plan — Workstation 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)

Section III — Project Approach and Work Schedule

Work Plan — Workstation 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

Section III — Project Approach and Work Schedule

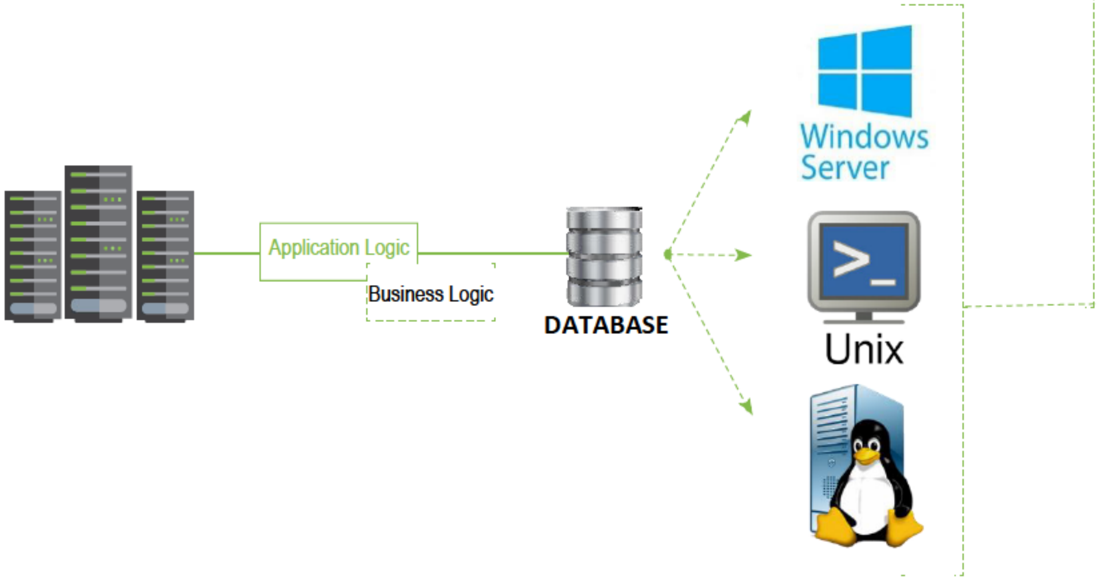
Work Plan — Server Configuration | Operating System Review

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 DISA 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 County's preferred framework or the NIST framework

- User provisioning
- System and data backup
- Disaster recovery
- Change management
- Patch management
- Data classification

Section III — Project Approach and Work Schedule

Work Plan — Physical Security Assessment

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

Section III — Project Approach and Work Schedule

Work Plan — Mobile Device 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

Understand the process for managing mobile devices distributed by the organization

Review the mobile device security policy

Assess the configurations and OS versions of a sample of mobile devices

Review the policy configuration of the MDM solution, including (where applicable):

- Application inventory and restrictions, such as whitelisting and blacklisting
- Authentication
- Automated detection and response to policy violations
- Data encryption
- OS version | rooted device restrictions
- Public WiFi | USB port restrictions
- Remote wipe and lock
- Software updates
- User and application access to hardware and OS

Section III — Project Approach and Work Schedule

Work Plan — VPN Configuration Review

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

Pre-Analysis

Our review will begin by interviewing the VPN administrator(s) to gain an understanding of County's IT environment and how the VPN has been configured to work within it.

VPN
Users
All devices

Analysis

To analyze the security of Client's VPN, we will:

Assess the firmware version scan of

Perform a vulnerability

the VPN device

Review configuration manually

Assess use of insecure protocols

Ensure compliance with change management

Assess user provisioning for new, terminated, and transferred users, including employees, consultants, and third-party contractors

Section III — Project Approach and Work Schedule

Work Plan — VPN Configuration Review (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 Client'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

Section III — Project Approach and Work Schedule

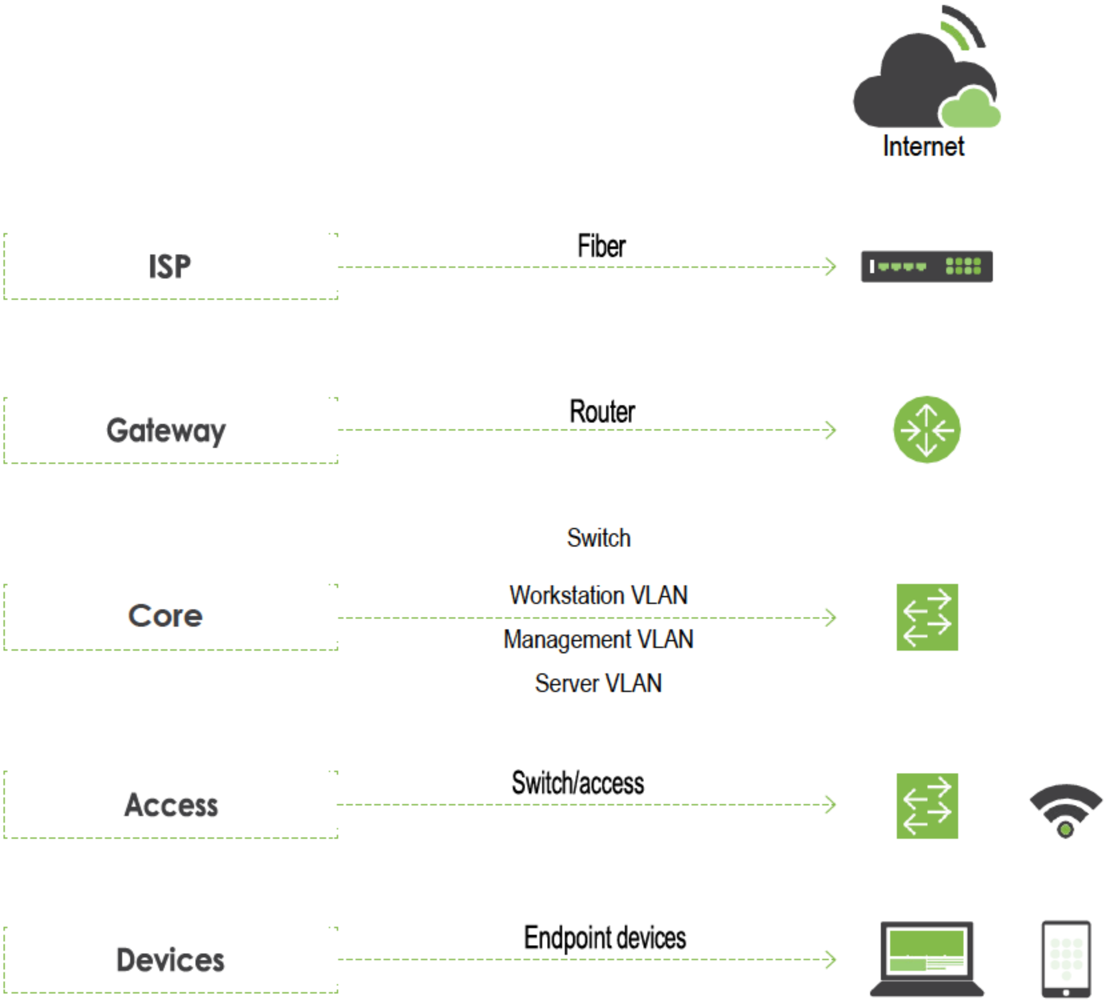
Work Plan — Network Architecture Review

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:



Section III — Project Approach and Work Schedule

Work Plan — 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).

Routers are intelligently and securely configured and leveraged effectively

Unused ports are disabled

The external router does not forward private IPs, while the internal core does not forward connections originating from an Internet IP address

A choke VLAN exists and enforces an inspection point

All business unit servers are in separate VLANs

DNS is properly and securely configured

On internal networks, all route distribution is authenticated (e.g., between firewalls and core)

Management VLAN contains designated jump servers to access network device and firewall consoles

Routers are used to eliminate generic classes of undesired traffic before such traffic hits a firewall

Private IPs are used on the internal network

The external router bins unknown protocols not provisioned in the DMZs

Data center servers are protected by a separate firewall

External connections are facilitated via reverse proxies hosted in a DMZ

Workstations are separated into functional business units to prevent malware and information leakage

A separate network management VLAN exists, accessed off the core and protected by ACLs

Ports 8080 to 8090, rather than port 80, are used to publish intranet services

Section III — Project Approach and Work Schedule

Schedule

b. Provide a schedule that will complete the project 120 days after execution of contract (the 120 days after execution target is negotiable). This schedule should contain specific milestones and dates of completion which will be used to set schedules.

The chart below outlines each step in our HIPAA security 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. This timeline assumes a start date of Monday, April 3, 2023 and a completion date (based on the scope of services) of June 2, 2023.

HIPAA Security Risk Assessment	4.3-4.7	4.10-4.14	▼4.17-4.21	Resource
Milestone — Planning				
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
Milestone — HIPAA Compliance Assessment				
Privacy Rule		▨	▨	SC Consultants
Obtain and review all HIPAA Privacy policies and supporting procedures and forms		▨	▨	SC Consultants
Compare the 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
Breach Notification		▨	▨	SC Consultants
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

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

Section III — Project Approach and Work Schedule

HIPAA Security Risk Assessment	4.10-4.14	4.17-4.21	4.24-4.28	Resource
		▼	▼	
Security Rule	▨	▨		SC Consultants
Obtain and review all HIPAA Security Rule policies	▨	▨		SC Consultants
Compare the 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
Milestone – Technical Testing				
External Network Vulnerability Assessment and Penetration Test			▨	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
Web Application Assessment			▨	SC Consultants
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
Firewall Configuration Review			▨	SC Consultants
Interview firewall administrator			▨	SC Consultants County Staff
Analyze firewall configuration			▨	SC Consultants
Assess results of configuration analysis			▨	SC Consultants

▼ ◆

Section III — Project Approach and Work Schedule

Schedule (continued)

HIPAA Security Risk Assessment	5.1-5.5	5.8-5.12 ▼	Resource
Social Engineering	▨		SC Consultants
Determine type of phishing campaign and obtain the list of targets	▨		SC Consultants
Perform phishing techniques	▨		SC Consultants
Determine the value of obtained information and attempt to use it to exploit additional confidential information	▨		SC Consultants
Wireless Assessment	▨		SC Consultants
Identify controllers and SSIDs	▨		SC Consultants
Interview wireless network administrator	▨		SC Consultants County Staff
Perform wireless network scanning	▨		SC Consultants
Obtain and assess wireless or AP configuration	▨		SC Consultants
Perform manual penetration activities	▨		SC Consultants
Analyze results and review with wireless administrator	▨	✦	SC Consultants County Staff
Enterprise Application Assessments	▨		SC Consultants
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
Endpoint Security Assessment		▨	SC Consultants
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 benchmarks		▨	SC Consultants

▼ PROJECT STATUS MEETINGS ✦ WORK PRODUCT REVIEWS

Schedule (continued)

HIPAA Security Risk Assessment	5.15-5.19	5.22-5.26	Resource
Server Operating System Configuration Review	▨		SC Consultants
Assess County's build and configuration standards	▨		SC Consultants
Interview database 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 database administrator	▨		SC Consultants County Staff
Physical Security Assessment	▨		SC Consultants
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
Mobile Device Security Assessment		▨	SC Consultants
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's PM		▨	SC Consultants County PM
VPN Configuration Review		▨	SC Consultants
Interview VPN administrator, review logs, 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

Schedule (continued)

HIPAA Security Risk Assessment	5.22-5.26	5.29-6.2	Resource
Network Architecture Review	▨		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
Milestone — Reporting			
Draft Management Report		▨	SC Consultants
Review management report with County's Key Stakeholders		▨	Paul Ashe County Stakeholders
Review Final Report and Hold Exit Conference		▨	Paul Ashe County PM

▼ PROJECT STATUS MEETINGS ✦ WORK PRODUCT REVIEWS

Section III — Project Approach and Work Schedule

County Personnel Responsibilities

c. Identify the extent of County personnel involvement deemed necessary, including key decision points at each stage of the project.

County personnel involvement will be required throughout the engagement, including:

- Project manager and applicable staff to help during the planning phase and to respond to the client assistance memo
- Various staff to respond to interview requests during the HIPAA Compliance Assessment phase
- Project manager to review results of vulnerability scans
- Firewall administrator(s) to respond to interview requests
- Wireless network administrator(s) to respond to interview requests and review results of penetration tests
- Database administrator(s) to respond to interview requests and review results of penetration tests
- Physical security personnel to respond to interview requests
- Project manager to review policy configuration of the MDM solution
- VPN administrator to respond to interview requests and review results of penetration tests
- Network engineer to respond to interview requests and review results of assessment
- Project manager and County stakeholders to review management report and attend exit conference

Securance has made the following assumptions regarding 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 project manager 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

Section III — Project Approach and Work Schedule

Deliverables

d. Provide outline and/or samples from previous projects.

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 the findings and recommendations are understood, and to answer any questions that County may have. In addition, we will provide free technical support and advice throughout the remediation phase.

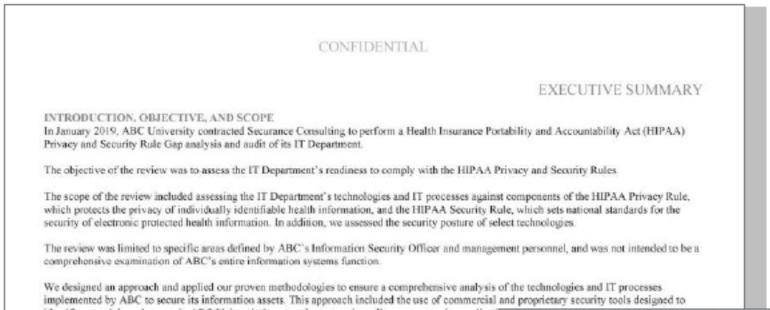
In the Appendix, we provide a sample HIPAA risk assessment report for County to review.

Management Report

Within one week of completing our fieldwork for the HIPAA security risk assessment, Securance will provide County with a board-ready management report tailored to its environment and needs and developed with input from County's stakeholders and IT management. Our analysis of the risks identified within County's environment will take into account its threat profile and the likelihood and impact of exploitation of existing vulnerabilities. The report 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. Comprised of two sections, the report will include an executive summary and a detailed project report, each of which is described below.

Executive Summary

The executive summary will outline the engagement's scope, approach, findings, and recommendations 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.



CONFIDENTIAL

EXECUTIVE SUMMARY

INTRODUCTION, OBJECTIVE, AND SCOPE

In January 2019, ABC University contracted Securance Consulting to perform a Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule Gap analysis and audit of its IT Department.

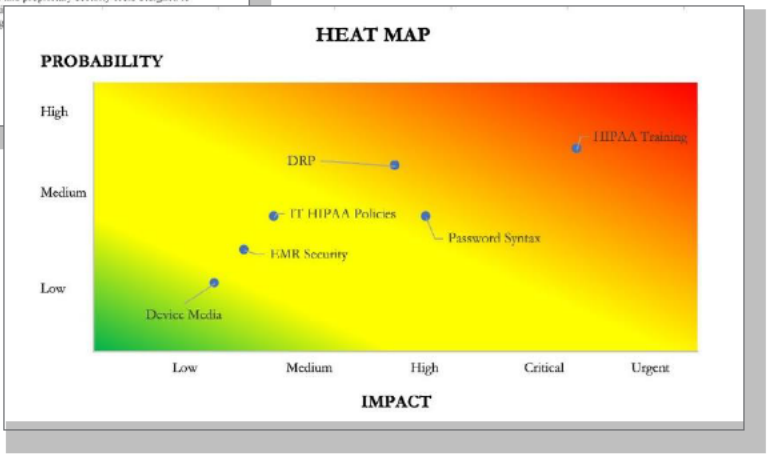
The objective of the review was to assess the IT Department's readiness to comply with the HIPAA Privacy and Security Rules.

The scope of the review included assessing the IT Department's technologies and IT processes against components of the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information, and the HIPAA Security Rule, which sets national standards for the security of electronic protected health information. In addition, we assessed the security posture of select technologies.

The review was limited to specific areas defined by ABC's Information Security Officer and management personnel, and was not intended to be a comprehensive examination of ABC's entire information systems function.

We designed an approach and applied our proven methodologies to ensure a comprehensive analysis of the technologies and IT processes implemented by ABC to secure its information assets. This approach included the use of commercial and proprietary security tools designed to identify potential weaknesses in ABC University's networks, network appliances, enterprise applicati
scope assessed were also compared to industry standards and our internal risk management knowledg

Remainder of this page left blank intentionally.

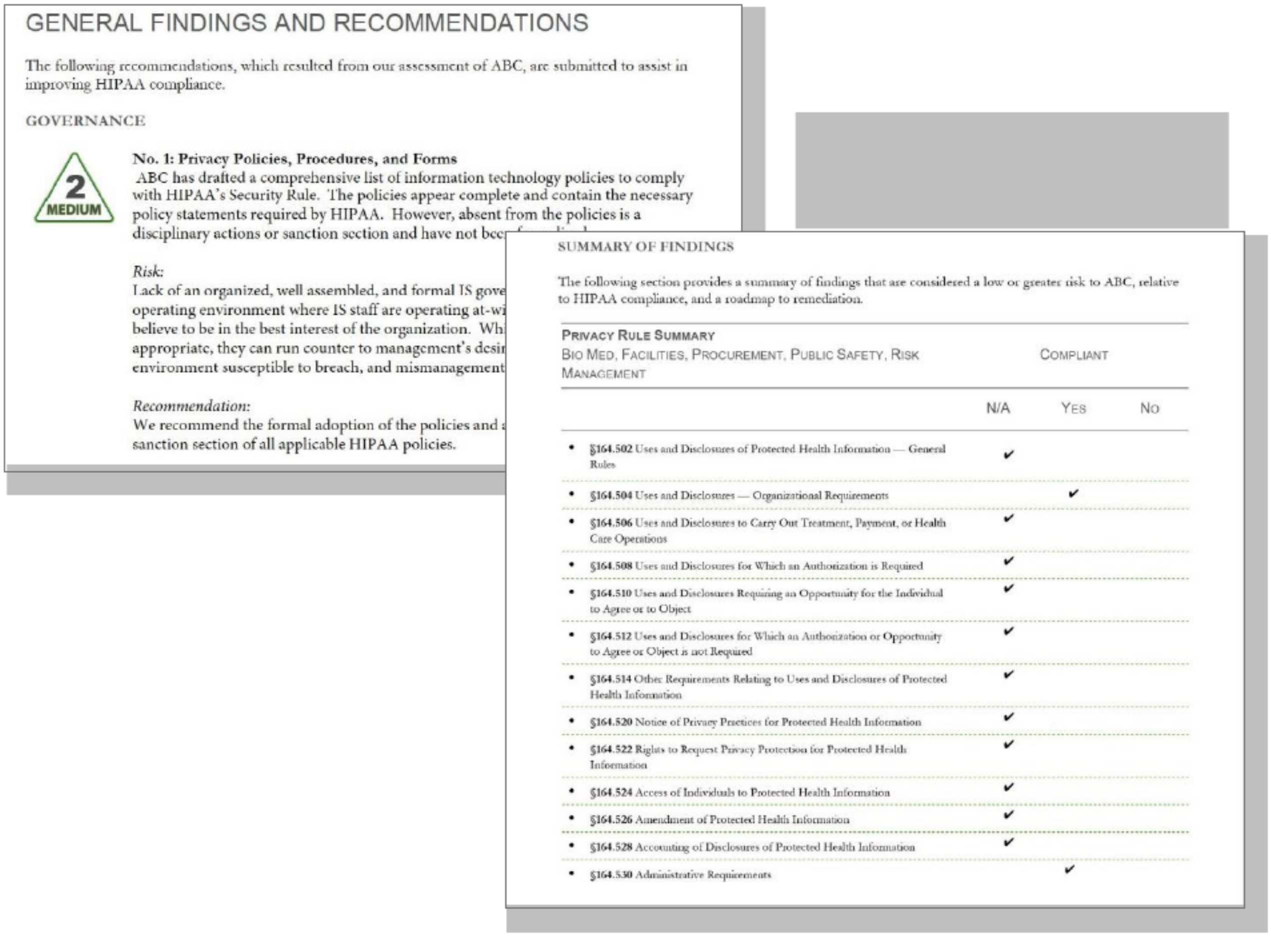


Section III — Project Approach and Work Schedule

Deliverables (continued)

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.



GENERAL FINDINGS AND RECOMMENDATIONS

The following recommendations, which resulted from our assessment of ABC, are submitted to assist in improving HIPAA compliance.

GOVERNANCE

No. 1: Privacy Policies, Procedures, and Forms
ABC has drafted a comprehensive list of information technology policies to comply with HIPAA's Security Rule. The policies appear complete and contain the necessary policy statements required by HIPAA. However, absent from the policies is a disciplinary actions or sanction section and have not bee

Risk:
Lack of an organized, well assembled, and formal IS gove
operating environment where IS staff are operating at-wi
believe to be in the best interest of the organization. Wh
appropriate, they can run counter to management's desi
environment susceptible to breach, and mismanagement

Recommendation:
We recommend the formal adoption of the policies and
sanction section of all applicable HIPAA policies.

SUMMARY OF FINDINGS

The following section provides a summary of findings that are considered a low or greater risk to ABC, relative to HIPAA compliance, and a roadmap to remediation.

PRIVACY RULE SUMMARY BIO MED, FACILITIES, PROCUREMENT, PUBLIC SAFETY, RISK MANAGEMENT	COMPLIANT		
	N/A	YES	NO
• **§164.502** Uses and Disclosures of Protected Health Information — General Rules	✓		
• **§164.504** Uses and Disclosures — Organizational Requirements		✓	
• **§164.506** Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations	✓		
• **§164.508** Uses and Disclosures for Which an Authorization is Required	✓		
• **§164.510** Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object	✓		
• **§164.512** Uses and Disclosures for Which an Authorization or Opportunity to Agree or Object is not Required	✓		
• **§164.514** Other Requirements Relating to Uses and Disclosures of Protected Health Information	✓		
• **§164.520** Notice of Privacy Practices for Protected Health Information	✓		
• **§164.522** Rights to Request Privacy Protection for Protected Health Information	✓		
• **§164.524** Access of Individuals to Protected Health Information	✓		
• **§164.526** Amendment of Protected Health Information	✓		
• **§164.528** Accounting of Disclosures of Protected Health Information	✓		
• **§164.530** Administrative Requirements		✓	

Technician's Report (Technical Security Testing Only)

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.

Section III — Project Approach and Work Schedule

Deliverables (continued)

> The confidentiality of the analysis and final reports must be maintained at all times. Proposers must discuss how confidentiality is maintained during the analysis process.

Securance consultants regularly handle sensitive client information when conducting assessments. To ensure all sensitive information is handled properly, Securance will use Box.com as a secure document sharing portal. Information stored in Box.com is securely accessed via identity and authentication, document watermarking, reporting and usage logs, device trust, and the use of an administrative console. The data is encrypted in transit using high-strength TLS encryption and at rest via 256-bit AES encryption.

Additional security systems in place to safeguard County's data include:

- All Securance consultants will execute a confidentiality agreement.
- Consultants will perform all activities on a company-issued workstation that:
  - Are configured using whole disk encryption
  - Have local firewalls enabled
  - Have current a anti-virus solution
- In addition to using Box.com, when it is essential for Securance and County to share sensitive information, our team will:
  - Encrypt any sensitive information shared via email
  - Encrypt and password-protect any reports containing sensitive information
  - Use passwords that meet or exceed standard complex password standards
  - Only communicate passwords via telephone or under separate email cover

To ensure no disruption to County's systems, when Securance performs penetration testing:

- All vulnerability assessments and penetration testing will be performed:
  - After normal business hours or at a time requested by County's IT personnel
  - Using a policy that ensures no disruption to the network
  - More aggressive scanning procedures will only be performed after we obtain explicit approval from County's PM
- Procedures with the potential to be disruptive will be performed using manual techniques at a guarded pace
  - IT Management will be asked to monitor network and system performance and to notify Securance if performance becomes unacceptable
  - In the unlikely event of network or system disruption, the active procedures will be terminated
- Securance will not attempt exploitation of mission-critical systems or resources without explicit written permission from County's PM
- Securance will log all actions, including changes to system settings and configurations, taken against compromised systems
- After completing our penetration testing procedures, we will restore all settings and configurations to their initial values

Section III — Project Approach and Work Schedule

Project Organization

e. Provide project organization and staffing, including an organizational chart identifying each member of the firm involved with the project. The chart shall show the organizational structure of the team and the specialty or position of each team member.

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, CMMC-AB RP (pending), CPA, HCISPP (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 HIPAA security risk assessment procedures and all technical testing based on County's environment
- Execution of the HIPAA security risk assessment and technical testing in an efficient manner
- Identification of risks, vulnerabilities, compliance gaps, exposures, and other opportunities for improvement

Senior HIPAA Consultants

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

Chris Bunn, CHP, CISSP, CMMC-AB RP

Ibrahim Badrawi, CCNA, CVA, Security +

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

- Plan, coordinate, and execute the HIPAA security risk assessment and technical testing based on County's environment
- Identify risks, vulnerabilities, compliance gaps, and exposures, and other opportunities for improvement
- Prepare assessment reports, status reports, and other deliverables for review with County's PM
- Ensure he is notified of any project issues or delays

While all three Senior HIPAA Risk Consultants will work on most aspects of the engagement, they each have specific expertise. Chris Bunn's specific expertise is in HIPAA security risk compliance, while Ray Resnick's and Ibrahim Badrawi's specific expertise lies in supporting technical testing, physical security, assessments, and social engineering.

Section III — Project Approach and Work Schedule

Software | Quality Control | Sample Report

f. Discuss the type of any software that is anticipated to be used in the planning process.

In addition to manual testing, Securance will use automated tools during the vulnerability scan and penetration test phases of the project. Our most commonly used toolset includes:

- Nmap
- Nessus
- Qualys
- OWASP Zap
- Burp Suite
- NStalker
- Metasploit
- Core Impact
- Canvas

Use of additional tools may be used according to the nature of the task.

g. Describe the level of quality control that you recommend for this project. What characteristics define this level of quality?

Experience Drives Our Quality

Quality is an integral part of everything we do. Over the past 21 years, we have striven to integrate new concepts and methods into our workflows, including making real-time corrections to our processes to eliminate problems as soon as we detect them. Our team's combined century of experience will help ensure County receives the highest level of quality. All Securance projects are led by senior IT consultants with at least 20 years' experience. Their work is reviewed by the engagement manager, and the final product is reviewed by an executive independent of the project.

We certify that our work product will meet or exceed the requirements of County's internal standards.

In our experience, the most common roadblocks to successful project completion and client satisfaction are project setbacks due to delays in receipt of requested documentation and | or disagreement over project findings. To avoid these roadblocks, Securance will provide the County's PM with bi-weekly status reports, which will contain a section detailing open items and pending requests for information. We also document all project findings and related evidence in an issue tracker, which we will regularly share with County to avoid unwanted surprises at the end of the engagement.

SECTION IV — COST OF SERVICE

Cost Pages

Securance has provided Year-1 itemized pricing for the major aspects of this project in the table below.

Project Scope Item	Line Item Fee
HIPAA Compliance Risk Assessment (Privacy Rule and Security Rule Assessments) (5 departments, 22 locations)	$17,360
HIPAA Compliance Risk Assessment (Breach Notification) – Value Add	$4,960
External Vulnerability Assessment and Penetration Test (12 IPs) — Value Add	$1,488
Internal Vulnerability Assessment and Penetration Test (24 Ips in 2023 and 2024. 60 IPs in 2025, 2026, and 2027)	$4,960
Physical Security Assessment (5 locations)	$2,480
Web Application Testing (6 applications)	$2,976
Enterprise Application Testing	$7,440
Wireless Network Assessment (2 wireless networks, 2 SSIDs, 2 physical locations)	$1,984
Server | Operating System Configuration Review (4 operating systems)	$2,728
Workstation Configuration Review (ISD: 1800 endpoints, HSD: 1520 endpoints)	$1,488
Firewall Configuration Review (ISD: 1, HSD: 1, plus an additional in Azure)	$3,720
VPN Configuration Review (ISD: 2 appliances, HSD: 2 appliances)	$2,976
Mobile Device Assessment (12 devices, 7 locations, 2 controllers)	$2,728
Social Engineering (Phishing — ISD: 10 targets, HSD: 3 targets) — Value Add	$6,200
Network Architecture Review	$1,984
Reporting	$2,976
Travel	Included
Independent Project Review*	Included
Subtotal	$68,448
Value Add Price Reduction	($12,648)
Total – Year 1 (2023)	$55,800

Section IV —Cost of Service for Year 2, Year 3, Year 4, and Year 5

Total cost for the above scope of services in Year 2 (2024 Risk Assessment)………… $58,032
Total cost for the above scope of services in Year 3 (2025 Risk Assessment)………… $69,453
Total cost for the above scope of services in Year 4 (2026 Risk Assessment)………… $75,009
Total cost for the above scope of services in Year 5 (2027 Risk Assessment)………… $81,010

**Each assessment completed by Securance is reviewed by a consultant independent of the project, in order to ensure that the engagement thoroughly addresses all scope items, all observations are factual and appropriately documented, recommendations are feasible and customized to County, and all assessment components adhere to the firm's quality control standards.*

Section IV — Cost of Service Assumptions

Securance's proposed fees are based on the information that has been made available to us and on our understanding of the engagement. 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 $124, 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.

Payment Terms

Securance will submit an invoice after delivering a draft management report. All fees are due within 30 days following receipt of invoice. Securance will deliver the final management report following receipt of payment.

Section IV — Cost of Service

Added Value

Securance will provide County with three value-added deliverables. Each of the deliverables described in the table below is intended to help County continually improve its overall information security posture long after this engagement is over.

- HIPAA Breach Notification Rule Compliance Assessment

  As part of our breach notification assessment process, we will determine if the organization is compliant with HIPAA breach notification standards; policies are aligned with standards; and a breach notification process is in place.

- External Network Vulnerability Assessment | Penetration Testing

  We will provide the requested vulnerability assessment and penetration test of the external network at no

- Social Engineering

Required scope item provided at no cost to County. We will prove the adequacy of or demonstrate the need for improved security awareness training by conducting phishing social engineering exercises.

Exhibit B. County's Insurance Requirements

(Template 5 – Rev 2024 May 20)

With respect to performance of work under this Agreement, Contractor shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a Waiver of Insurance Requirements. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

County reserves the right to review any and all of the required insurance policies and/or endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve Contractor from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

1. Workers Compensation and Employers Liability Insurance

   a. Required if Contractor has employees as defined by the Labor Code of the State of California.

   b. Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.

   c. Employers Liability with minimum limits of $1,000,000 per Accident; $1,000,000 Disease per employee; $1,000,000 Disease per policy.

   d. Required Evidence of Insurance: Certificate of Insurance.

If Contractor currently has no employees as defined by the Labor Code of the State of California, Contractor agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

2. General Liability Insurance

   a. Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) form CG 00 01.

   b. Minimum Limits: $1,000,000 per Occurrence; $2,000,000 General Aggregate; $2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance. If Contractor maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by Contractor.

   c. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds $100,000, it must be approved in advance by County. Contractor is responsible for any deductible or self insured retention and shall fund it upon County’s written request, regardless of whether Contractor has a claim against the insurance or is named as a party in any action involving the County.

d. **"County of Sonoma, its Officers, Agents, and Employees"** shall be endorsed as additional insureds for liability arising out of operations by or on behalf of the Contractor in the performance of this Agreement.

e. The insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.

f. The policy definition of "insured contract" shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage including the "f" definition of insured contract in ISO form CG 00 01, or equivalent).

g. The policy shall cover inter-insured suits between the additional insureds and Contractor and include a "separation of insureds" or "severability" clause which treats each insured separately.

h. Required Evidence of Insurance: Certificate of Insurance.

3. Cyber Liability Insurance – Network Security & Privacy Liability Insurance

a. Minimum Limit: $2,000,000 per claim or per occurrence, $2,000,000.00 aggregate.

b. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Consultant in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, 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, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.

c. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

d. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

e. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

4. Cyber Liability Insurance – Technology Errors and Omissions Insurance

a. Minimum Limit: $2,000,000 per claim or per occurrence, $2,000,000.00 aggregate.

b. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Consultant in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, 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, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.

c. The Policy shall include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the County in the care, custody, or control of the Consultant. If the Consultant maintains broader coverage and/or higher limits than the minimums shown above, the Entity requires and shall be entitled to the broader coverage and/or the higher limits maintained by the contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the Entity.

d. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

e. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

f. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

5. Standards for Insurance Companies

Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

6. Documentation

a. All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Contractor agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.

b. The name and address for Additional Insured endorsements and Certificates of Insurance is:

County of Sonoma, its Officers, Agents, and Employees
Attn: DHS – Contract & Board Item Development Unit
1450 Neotomas Avenue, Suite 200
Santa Rosa CA 95405
Email: DHS-Contracting@sonoma-county.org

c. Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists, at least ten (10) days before expiration or other termination of the existing policy.

d. Contractor shall provide immediate written notice if: (1) any of the required insurance policies is terminated; (2) the limits of any of the required policies are reduced; or (3) the deductible or self-insured retention is increased.

e. Upon written request, certified copies of required insurance policies must be provided within thirty (30) days.

7. Policy Obligations

Contractor's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

8. Material Breach

If Contractor fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. County, at its sole option, may terminate this Agreement and obtain damages from Contractor resulting from said breach. Alternatively, County may purchase the required insurance, and without further notice to Contractor, County may deduct from sums due to Contractor any premium costs advanced by County for such insurance. These remedies shall be in addition to any other remedies available to County.