JMU
JAMES MADISON
UNIVERSITY.

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU7145**

This contract entered into this 25th day of March 2025, by Securance, LLC., hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

WITNESSETH that the Contractor and the Purchasing Agency, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From April 1, 2025 through March 30, 2026 with nine (9) one-year renewal options.

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposal FDC-1220 dated December 17, 2024:
  (a) The Statement of Needs,
  (b) The General Terms and Conditions,
  (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
  (d) Addendum One, dated January 10, 2025;
  (e) Addendum Two, dated January 16, 2025.

(3) The Contractor's Proposal dated January 27, 2025 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
  (a) Negotiations Summary, dated March 17, 2025.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:	PURCHASING AGENCY:
By: DocuSigned by: Gillian Tedeschi 1215A67F57C6... (Signature)	By: (Signature)
Gillian Tedeschi (Printed Name)	Doug Chester (Printed Name)
Title: Vice President	Title: Buyer Senior

Rev. 5/12/21

JAMES MADISON
UNIVERSITY.

RFP # FDC-1220
Information Technology Security Auditing Services
Negotiation Summary for Securance, LLC.
March 17, 2025

1. Parties agree that items within this Negotiation Summary modify RFP #FDC-1220 and the Contractor's response to RFP #FDC-1220 and that this Negotiation Summary takes precedence in conflict.

2. Contractor agrees that all exceptions taken within their initial response to RFP #FDC-1220 that are not specifically addressed within this negotiation are null and void.

3. Contractor hereby rescinds confidentiality of its entire proposal dated January 27, 2025 and all subsequent negotiations.

4. The pricing schedule is as follows:

Pricing for Auditing Services	Off-site	On-site*
External Vulnerability Scanning	$137.75	$141.38
Wireless Network Assessment	$137.75	$141.38
Firewall and Router Security Assessment	$137.75	$141.38
Server Configurations Assessment	$137.75	$141.38
Database Architecture Security Assessment	$137.75	$141.38
Network Scanning Process Assessment	$137.75	$141.38
Web Application Security Assessment	$137.75	$141.38
Active Directory Security Assessment	$137.75	$141.38
Penetration Testing	$137.75	$141.38
Telecommunications	$137.75	$141.38
(flat fee hourly rate that includes all billables/travel)		

5. The University may also request that these services be provided as a fixed-fee project, as would be mutually agreed to prior to services being rendered, with deliverables billed upon completion of milestones.

6. The University may also request that these services be provided as a monthly subscription service, as would be mutually agreed to prior to services being rendered, with deliverables determined by monthly service requirements.

7. Upon completion of each Statement of Work, the Contractor shall submit a SWaM subcontractor usage report in accordance with RFP Special Term and Condition J: Small Business Subcontracting and Evidence of Compliance. Reports shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807 or swamreporting@jmu.edu.

8. Contractor has disclosed all potential fees. Additional charges will not be accepted without mutual written agreement between parties, e.g., contract modification and/or change order.

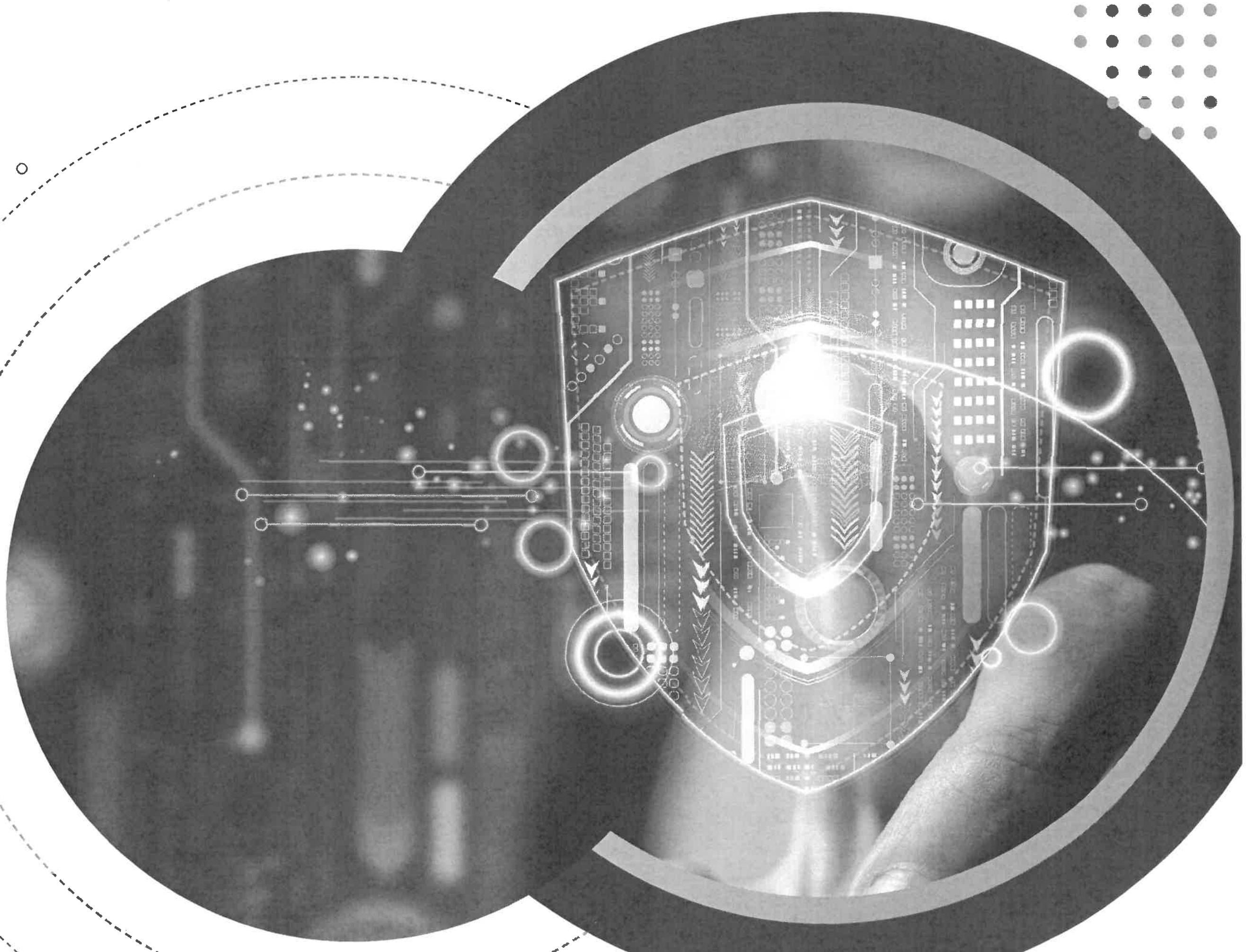
JANUARY 30, 2025

CLICK TO LISTEN

JAMES MADISON UNIVERSITY

RFP #FDC-1220

INFORMATION TECHNOLOGY SECURITY AUDITING SERVICES [REDACTED COPY]



Contact for RFP Response:

Shawn Johnson
Proposal Manager
SJohnson@securanceconsulting.com
877.578.0215 ext. 115

www.securanceconsulting.com

SECURANCE CONSULTING
the advantage of insight

SECURANCE CONSULTING

January 30, 2025

Doug Chester, Buyer Senior
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Dear Doug:

Thank you for considering Securance Consulting for James Madison University's (JMU's) upcoming information technology security auditing services. We have been a party to a master services agreement with JMU since 2018 and are pleased at the opportunity to renew our partnership.

Securance is an expert cybersecurity firm with more than 23 years of experience. We have the breadth of expertise to help JMU's Audit and Management Services (AMS) add value to the university through on-demand, independent assessments and insightful guidance for improvement. **We want to partner with you!** Through our collaboration with AMS and IT staff, JMU will benefit from our:

- **Senior IT Audit Consultants.** Our team of key consultants, which I will lead, has a combined 120 years of experience — 26 or more years each.
- **Education-Sector Expertise.** Securance has provided IT security services to dozens of educational institutions at all levels and understands their unique needs and challenges, including protecting student data in compliance with the Gramm-Leach-Bliley Act (GLBA).
- **Efficient Execution.** We will leverage our experience in the higher education sector to provide JMU with a board-ready draft report within one week of completing fieldwork for each audit.
- **Proven Track Record**. Securance has completed more than 3,000 IT audits and other security assessments during our two decades of service. We have completed all projects on time and within budget, and we will do the same for this engagement.
- **Proprietary Artificial Intelligence (AI) Tool.** We leverage AI to identify and predict risks, security weaknesses, compliance violations, and even potential attacks. We use generative AI (GenAI) and large language models (LLMs) to focus our approach to assessments and cybersecurity services on the most pertinent risks to our clients' technologies.

On the next page is a small sample of projects similar in scope to JMU's.

Client	Project(s)	Contract Value	Description	Performance Period
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

We acknowledge that Securance may not be the lowest-priced bidder for the services required by JMU. However, our services represent a superior value when compared to those offered at a lower cost by our competitors. From the detailed nature of our assessment to the comprehensiveness of our deliverables and the in-depth knowledge transfer we will conduct post-assessment, JMU will not find a firm whose analyses and results are more accurate and exhaustive than ours. Discussions with our clients over the past 23 years have confirmed that our slightly higher upfront costs represent significant long-term savings.

Thank you again for including Securance in your evaluation process. If you have any questions after reviewing our proposal, please do not hesitate to contact me.

Professional regards,

Paul Ashe, CPA, CISA, CISSP, CMMC-AB RP, HCISPP

President

We want to partner with you!

TABLE OF CONTENTS

23+ YEARS

Securance has more than 23 years of experience providing IT audit services similar in scope to those sought by James Madison University.

EXECUTIVE-LEVEL CONSULTANTS

Our executive-level consultants have provided vulnerability scans, penetration tests, and other technical assessments for clients such as [redacted]

EXTRA VALUE

Few firms are as dedicated to their clients as Securance will be to you. We will invest the time and effort necessary to learn JMU's IT environment and organizational objectives. Then we will use that understanding to conduct thorough IT audits and deliver actionable guidance for improvement.

This proposal contains confidential material proprietary to Securance Consulting. The material, ideas, and concepts contained herein are to be used solely and exclusively to evaluate the capabilities of Securance Consulting to provide assistance to James Madison University (JMU). This proposal does not constitute an agreement between Securance Consulting and JMU. Any services Securance Consulting may provide to JMU will be governed by the terms of a separate written agreement signed by both parties. All offers to provide professional services are valid for 60 days.

REQUIREMENTS MATRIX

Securance has formatted our proposal according to JMU's requirements. Below, we summarize the contents of our proposal:

RFP Section	Requirement	Page No.
IV. Statement of Needs C.	1. Describe your company's plan to provide certified professional staff to perform a wide range of IT audits of various IT activities and processes under the direction of the Director or staff of AMS.	3
	2. Describe your company's history in working with any institutions of higher education, especially those within the Commonwealth of Virginia.	32
V. Proposal Preparation and Submission: A. General Proposal Instructions	2. Should the proposal contain proprietary information, provide one (1) redacted copy of the proposal and all attachments with proprietary portions removed or blacked out. This copy should be clearly marked "Redacted Copy" on the front cover.	Separate file
	4.a. Proposals shall be signed by an authorized representative of the Offeror.	Cover letter
	4.c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, sub letter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and subletter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements.	Table of Contents
V. Proposal Preparation and Submission: B. Specific Proposal Instructions	1. Return RFP cover sheet and all addenda acknowledgements, if any, signed and filled out as required.	2
	2. Plan and methodology for providing the goods/services as described in Section IV. Statement of Needs of this Request for Proposal.	3
	3. A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.	30
	4. Offeror Data Sheet, included as Attachment A to this RFP.	51
	5. Small Business Subcontracting Plan, included as Attachment B to this RFP.	52
	6. Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution.	54
	7. Proposed Cost. See Section X. Pricing Schedule of this Request for Proposal.	55

1. RFP COVER SHEET | ADDENDA ACKNOWLEDGMENT

Return RFP cover sheet and all addenda acknowledgements, if any, signed and filled out as required.

REQUEST FOR PROPOSAL

RFP# FDC-1220

Issue Date: **December 17, 2024**

Title: **Information Technology Security Auditing Services**

Issuing Agency:
Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on January 21, 2025 for Furnishing The Services Described Herein. (See Special Terms & Conditions "D. Late Proposals")

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, SUBMITTED IN eVA, OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Doug Chester, Buyer Senior, Procurement Services, chestefd@jmu.edu; 540-568-4272; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.
In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:
Securance LLC
13916 Monroes Business Park, Suite 102
Tampa, FL 33635

By: ____________________
(Signature)

Name: Paul Ashe
(Please Print)

Date: 01.27.2025

Title: President

Web Address: securanceconsulting.com

Phone: 877.578.0215

Email: pashe@securanceconsulting.com

Fax #: NA

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 ✓ #2 ✓ #3____ #4____ #5____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
☐ YES; ☐ NO; *IF YES* ⇒⇒ ☐ SMALL; ☐ WOMAN; ☐ MINORITY *IF MINORITY:* ☐ AA; ☐ HA; ☐ AsA; ☐ NW; ☐ Micro

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against an offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

Rev. 9/2/2024

2. SECURANCE PLAN AND METHODOLOGY

- Plan and methodology for providing the goods I services as described in Section IV. Statement of Needs of this Request for Proposal.

Understanding of the Scope

We understand that the audits Securance will be asked to perform may include but will not necessarily be limited to those listed below. We have included methodologies for some of the assessment tasks on the following pages. Additional methodologies can be provided upon request.

PLANNING ACTIVITIES

- Kickoff Meeting
- Establish Rules of Engagement
- Create I Share Client Assistance Memo

IT SECURITY AUDITS

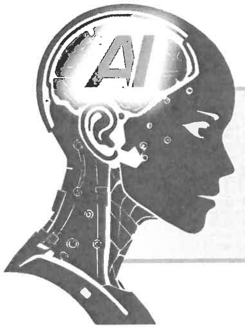
- External Network Vulnerability Scanning I Penetration Testing
- Wireless Network Assessment
- Firewall I Router I Server Configuration Review
- Database Assessment
- Web Application Assessment
- Active Directory Security Assessment
- Telecommunications (VoIP) Assessment

POST-AUDIT ACTIVITIES

- Board-Ready Management Report
- Remediation Retesting (If Required)

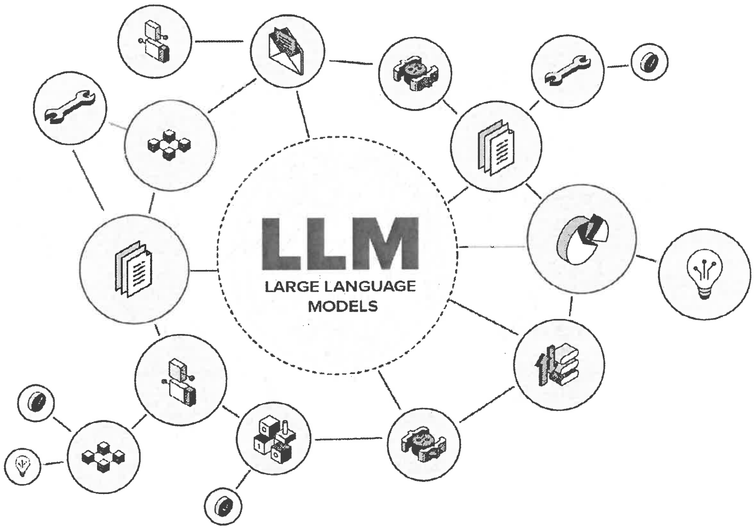
2. SECURANCE PLAN AND METHODOLOGY

Risk-Based IT Audits Powered by AI



Securance is **the first and only IT audit firm** to use generative AI (GenAI) and large language models (LLMs) to enhance its approach to client-focused assessments.

GenAI and LLMs can transform how businesses across industries gather and analyze information, predict outcomes, and make better decisions. Cybersecurity is no exception. At Securance, we use LLMs to identify potential risks based on a client's technologies, IT processes, and industry. We apply this information to focus our approach and methodologies when conducting IT audits.



LLMs consider billions of parameters and ingest massive amounts of data from sources such as the Internet, Common Crawl, which collects data from more than 50 billion web pages, and Wikipedia, with approximately 57 million pages. While not perfect, LLMs have a remarkable ability to make predictions based on a relatively small number of prompts, or inputs. GenAI uses LLMs to produce content based on human-language prompts that provide clarity and context.

2. SECURANCE PLAN AND METHODOLOGY

Risk-Based IT Audits Powered by AI

Securance's program leverages OpenAI's GPT-4o model. With 1 trillion parameters, GPT-4o can identify patterns from multimodal data, generate natural and readable output, and perform complex tasks. We use GPT-4o to deliver maximal value to our clients via customized methodologies, targeted assessments, and actionable recommendations to prevent security breaches. During an initial co-development and planning session, we gather information about the client, its technology environment, and its internal audit or IT organization.

We use this data to adjust our input prompts, which include:

- The organization's industry.
- The organization's size.
- The security framework(s) in place.
- The security tools in place.
- Whether the organization has a security operations center (SOC) monitoring its network.
- Whether the organization has an internal audit department.

Securance does not include confidential, proprietary, or sensitive data from our clients in our prompts.
Clients can opt out of participating in our private LLM if they choose.

Based on the input prompts, our LLMs and GenAI produce information that informs our assessment approach. Securance's model can even predict cyber breaches, events, and failures and their consequences. Predictions may include the potential for:

- Failures in IT process controls.
- Network, system, and/or application breaches based on the client's cybersecurity profile.
- End-user security failures and phishing attacks.
- Inappropriate access to data or systems by end users.

Harnessing the power of GenAI, Securance provides clients with accurate results, tailored recommendations, and unique advantages that other security firms cannot match. The benefits of a Securance assessment include:

- Comprehensive risk profile.
- Predictive risk analysis, including industry- and technology-specific risks.
- Recommendations to prevent costly network and system breaches.

To learn how we put this into practice, please review our selected detailed technical methodologies on the following pages. Other methodologies can be provided upon request.

External | Internal Network Vulnerability Assessment and Penetration Testing

[redacted]

2. SECURANCE PLAN AND METHODOLOGY

External | Internal Network Vulnerability Assessment and Penetration Testing (continued)

[redacted]

External | Internal Network Vulnerability Assessment and Penetration Testing (continued)

[redacted]

2. SECURANCE PLAN AND METHODOLOGY

External | Internal Network Vulnerability Assessment and Penetration Testing (continued)

[redacted]

2. SECURANCE PLAN AND METHODOLOGY

[redacted]

External | Internal Network Vulnerability Assessment and Penetration Testing (continued)

[redacted]

External I Internal Network Vulnerability Assessment and Penetration Testing (continued)

[redacted]

External | Internal Network Vulnerability Assessment and Penetration Testing (continued)

[redacted]

2. SECURANCE PLAN AND METHODOLOGY

Wireless Network Assessment

Securance assesses the configuration and security of on-premise controller, cloud-based controller, and access point-based wireless networks. Our consultants will interview the wireless network administrator and review the following security controls:

[redacted]

Wireless Network Assessment

Penetration Testing

[redacted]

Next-Generation Firewall Assessment

[redacted]

Next-Generation Firewall Assessment (continued)

[redacted]

Next-Generation Firewall Assessment (continued)

[redacted]

Web Application Assessment

[redacted]

Web Application Assessment (continued)

[redacted]

Web Application Assessment (continued)

[redacted]

2. SECURANCE PLAN AND METHODOLOGY

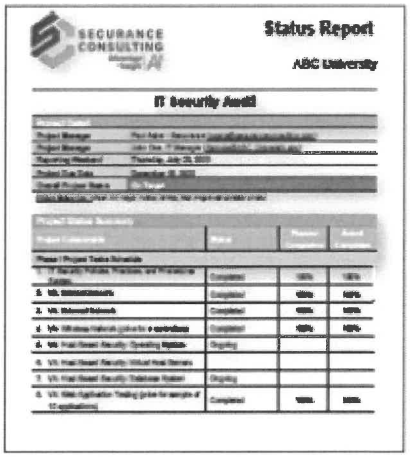
Project Management

Securance is dedicated to performing each audit as efficiently as possible. The assigned engagement manager (EM) will be responsible for ensuring project success by facilitating regular communication and providing status reports that will track progress, possible risks, and other pertinent information. Their specific responsibilities are outlined below:

OUR PROCESS

The EM will manage and oversee the entire project and be responsible for the following tasks:

- Project Kick-Off: Securance will hold a kick-off conference with JMU. During this meeting, we will introduce our project team, and define the project scope, objectives, timeline, and deliverables. We will also review the Client Assistance Request, which is a memo listing all documentation and interviews required to complete the assessment. We will establish the frequency of meetings and project status updates, key stakeholders, and lines of communication for both JMU and Securance.
- Work Plan: Within one week of receiving the notice to proceed, Securance will submit a detailed work plan for JMU's review and approval. Our work plan will include due dates for all deliverables, as well as intermediate milestones. We will update the work plan, as necessary, throughout the project.
- Status Reports: Throughout the engagement, JMU's project manager (PM) will receive project status reports that will identify the past week's completed tasks, planned tasks for the upcoming week, pending requests for information, and any issues and / or risks that have been identified, with actions taken to mitigate them.



SECURANCE CONSULTING

Status Report

ABC University

IT Security Audit

CLICK
ON THUMBNAIL
TO VIEW THE
STATUS REPORT

Project Management (continued)

OUR PROCESS (CONTINUED)

Shared Tasks

Securance's EM and key personnel will be responsible for the following tasks throughout each audit:

- **Issue and Risk Management:** Securance prioritizes issues by considering the following:
  - Overall impact an issue may have on the project.
  - Length of time the issue has been unresolved.
  - Criticality of the issue to JMU's IT environment.

These factors will be looked at as a whole and discussed with AMS to determine the ultimate priority of each issue. Additionally, as part of our status reports, we will document all project findings and related evidence in an "Issue Tracker" document that will also be shared with AMS. The use of this tracker helps to avoid unwanted surprises and I or disputes over findings.

- **Continuous Improvement:** We will invite JMU employees to shadow our consultants as they execute technical engagements. Additionally, to ensure continuous improvement of JMU's security objectives, our team will conduct a knowledge transfer session upon completion of the assessment.

THEIR APPROACH

- Limited communications related to project status.
- Findings not communicated until drafted.

THE SECURANCE WAY...

- Constant and consistent project communication.
- Immediate communication of urgent and critical findings.
- Confirmation of findings prior to drafting.

....DELIVERS EXTRA VALUE TO YOU.

- Securance provides exceptional project management expertise, leveraging 23 years of experience conducting more than 3,000 IT assessments, delivering project success on time and on budget.

2. SECURANCE PLAN AND METHODOLOGY

JMU Resources Needed to Complete the Project

When a contract or statement of work is executed, there are specific items Securance will need to perform the project. To ensure that JMU gets the most out of its partnership with Securance, we have provided an initial list of information, access requests, and documentation our experienced team will need to hit the ground running.

RESOURCES NEEDED

Access to JMU's Staff

- Adequate access to management and other key personnel for consultation and interviews.
  - Very little of these individuals' time will be taken, but some contact will be necessary
- Access to a project manager for scheduling interviews with appropriate JMU staff
- Access to technical staff (if needed) during the length of the technical testing (very little time needed)
- Access to staff who have been identified for interviews during the length of the project (approximately one hour each)
- Immediate access on a part-time basis to a cybersecurity staff member who can assist with questions (when needed)

Logical and Other Access Requests

- IP addresses relevant to the project (external and internal network penetration testing only)
- User IDs and passwords for web applications | operating systems (if needed)
- Authority to access network components and operating systems (as needed)

Rules of Engagement Memo (for vulnerability assessments and penetration testing only; please see an example on the next page)

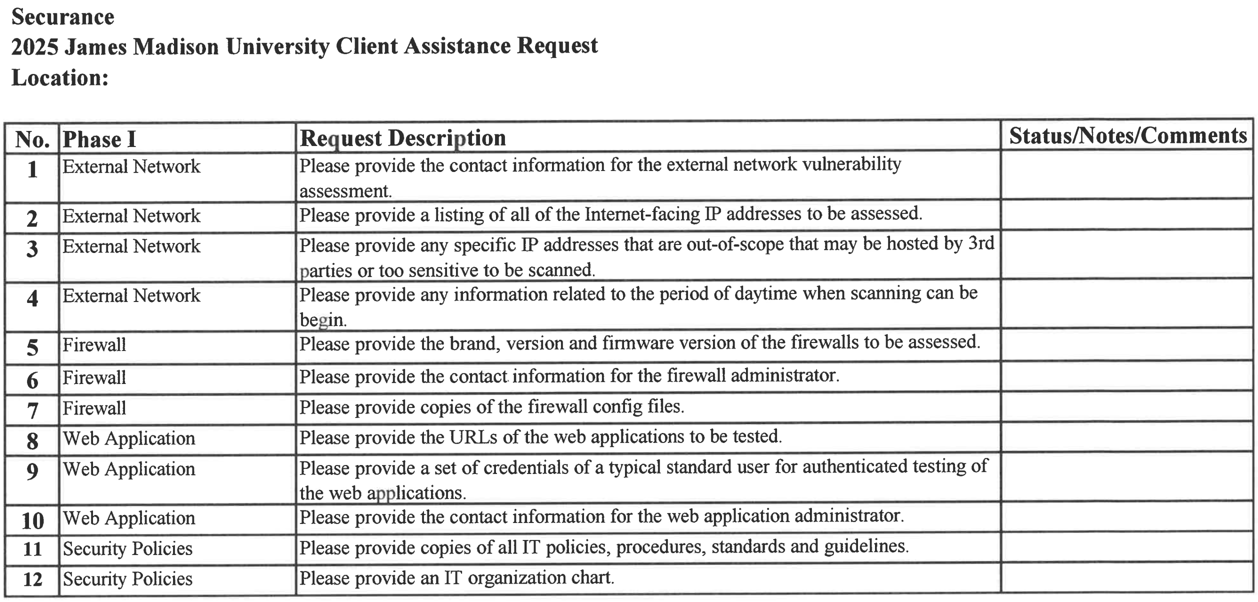
Client Assistance Request Summary (please see an example on pages 26–27)

Office Space for On-Site Work (As Needed)

- Identification badges or equivalent should be available on arrival (if needed)
- Lockable cabinet for documentation
- Workspace when on site

2. SECURANCE PLAN AND METHODOLOGY

JMU Resources Needed to Complete the Project (continued)



Securance
2025 James Madison University Client Assistance Request
Location:

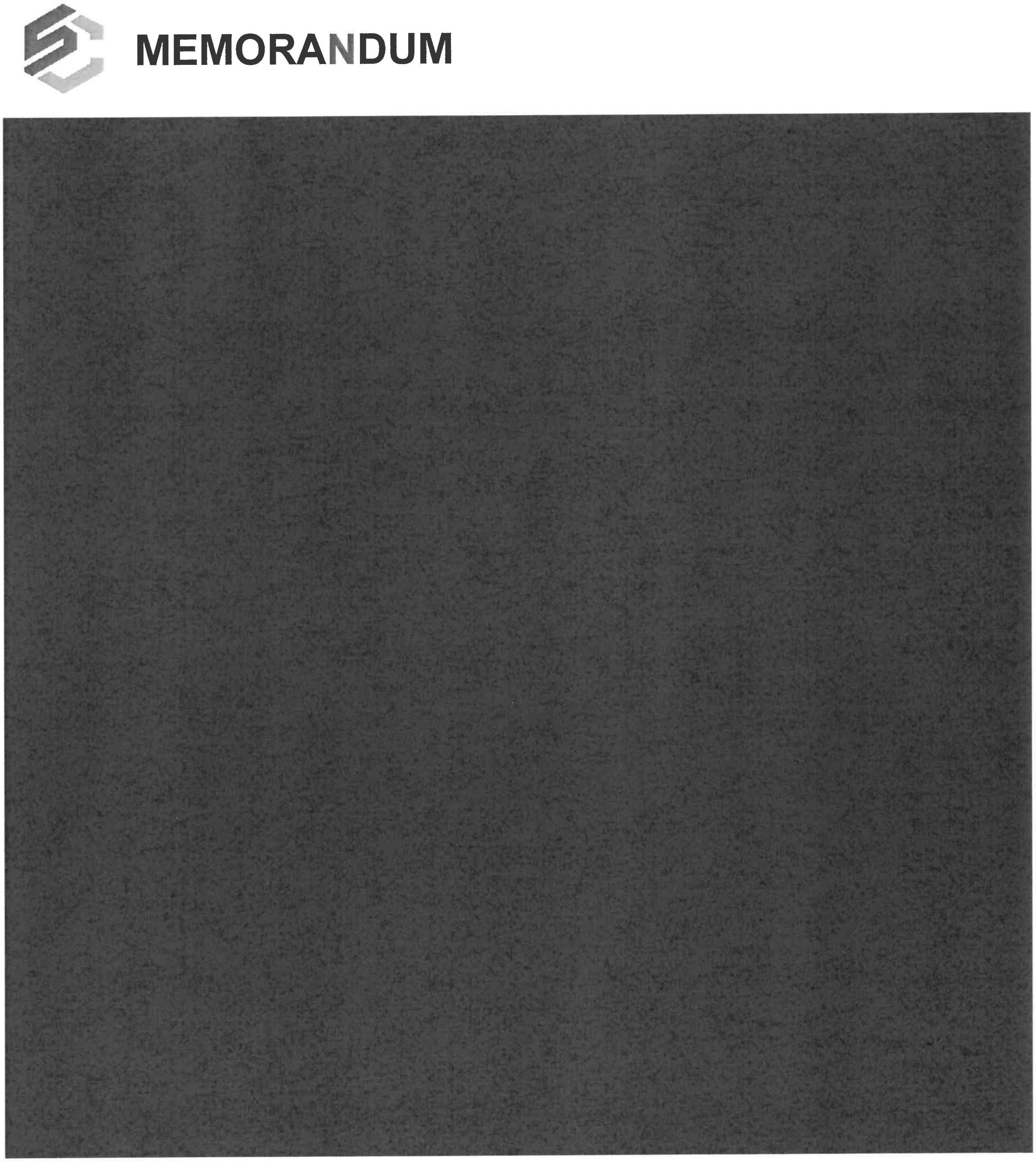
No.	Phase I	Request Description	Status/Notes/Comments
1	External Network	Please provide the contact information for the external network vulnerability assessment.	
2	External Network	Please provide a listing of all of the Internet-facing IP addresses to be assessed.	
3	External Network	Please provide any specific IP addresses that are out-of-scope that may be hosted by 3rd parties or too sensitive to be scanned.	
4	External Network	Please provide any information related to the period of daytime when scanning can be begin.	
5	Firewall	Please provide the brand, version and firmware version of the firewalls to be assessed.	
6	Firewall	Please provide the contact information for the firewall administrator.	
7	Firewall	Please provide copies of the firewall config files.	
8	Web Application	Please provide the URLs of the web applications to be tested.	
9	Web Application	Please provide a set of credentials of a typical standard user for authenticated testing of the web applications.	
10	Web Application	Please provide the contact information for the web application administrator.	
11	Security Policies	Please provide copies of all IT policies, procedures, standards and guidelines.	
12	Security Policies	Please provide an IT organization chart.	

JMU Resources Needed to Complete the Project (continued)

MEMORANDUM

[redacted]

JMU Resources Needed to Complete the Project (continued)



MEMORANDUM

[redacted]

Sample Deliverables

Management Report

Within one week of completing our fieldwork for each IT audit, Securance will provide JMU with a board-ready management report tailored to its environment and needs, and developed with input from the City's stakeholders and IT management. Our analysis of the risks identified within JMU'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 JMU's risk appetite. Comprising two sections, the report will include an executive summary and a detailed project report, each of which is described below.

[redacted]

During the engagement, if Securance identifies a vulnerability defined as urgent or critical by the Common Vulnerability Scoring System (CVSS), or any other risk that we feel needs immediate attention, our team will promptly notify JMU. Once JMU's staff has addressed the risk or threat, Securance will reassess it to validate remediation success.

Sample Deliverables (continued)

[redacted]

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

- A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.

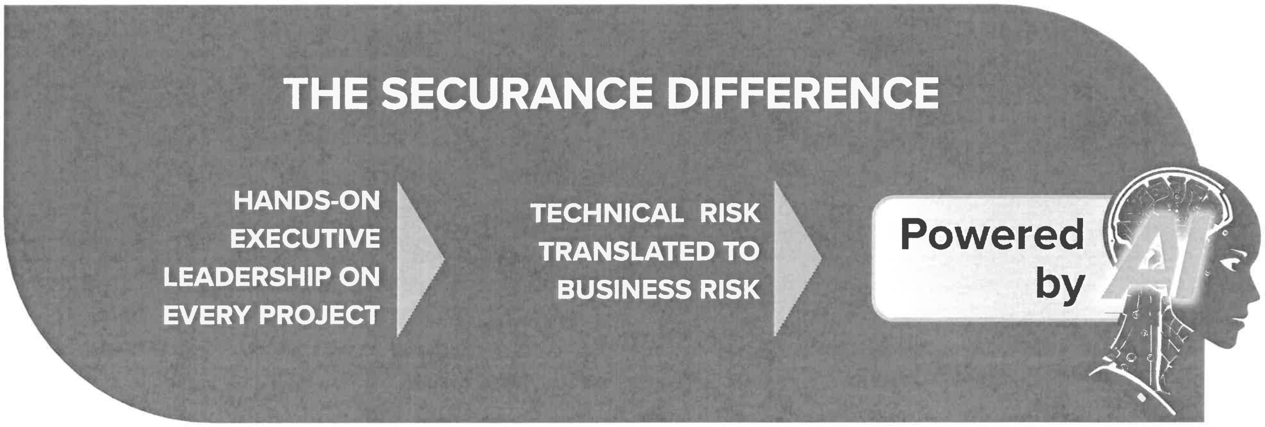
About Securance

More Than Two Decades of IT Audit Services

Securance is a 100-percent minority-owned limited liability company, certified as an 8(a), Small Disadvantaged Business (SDB), and Minority Business Enterprise (MBE). Paul Ashe, JMU's proposed engagement manager (EM), founded Securance in March 2002. Since then, we have performed more than 3,000 IT security assessments for clients in nearly every industry, including numerous higher-education clients, helping them to align their cybersecurity postures with their risk appetites.

Exclusively Staffed with Senior-Level IT Audit Professionals

To provide the highest-quality services, Securance only hires IT consultants with at least 15 years of professional experience. Their expertise in security assessments, compliance standards, and industry needs is our foundation. We tailor each project to the unique specifications required by our clients' IT environments, security and control standards, and business requirements. They are committed to clear and proactive communication and will work with all relevant JMU departments and staff to achieve the project objectives.



THE SECURANCE DIFFERENCE

HANDS-ON EXECUTIVE LEADERSHIP ON EVERY PROJECT

TECHNICAL RISK TRANSLATED TO BUSINESS RISK

Powered by AI

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

The Securance Difference

HANDS-ON EXECUTIVE LEADERSHIP ON EVERY PROJECT

A niche IT audit and cybersecurity and consulting firm, Securance was founded more than two decades ago by a group of executives from Big 4 accounting firms. Their vision was to provide highly specialized IT consulting services to clients in a wide range of industries, with unique advantages that only a small business could offer. Among these benefits are the caliber of our professional staff and the hands-on involvement of our executive team in client projects.

Larger firms use senior resources to lead their businesses but often turn much of the fieldwork on client projects over to less experienced consultants. This is not the case with Securance. **Our professional staff is limited to senior IT consultants with at least 15 — and, often, 30 or more — years of experience. Senior staff members do not just lead our projects; they execute them from cradle to grave.** Our firm's executives, such as founder and president Paul Ashe and security lead Ray Resnick, work alongside our staff consultants on every project.

TECHNICAL RISK TRANSLATED TO BUSINESS RISK

We have worked with hundreds of clients over the years and understand the disconnect that can occur when IT speaks one language and business another. An assessment report filled with technical jargon may be useful to a system administrator or engineer, but it provides little, if any, value to the C-suite. **Securance's reports are written in plain English that both technical and non-technical executives can understand.** We explain the potential adverse effect of each finding on business operations. This approach extends the value of our analysis beyond the IT department, helping senior management understand the risks and making our recommendations truly actionable.

Securance is the *only* IT audit firm that uses generative artificial intelligence (GenAI) and large language models (LLMs) to enhance its approach to identifying and assessing technology risks. Our proprietary GenAI technology uses OpenAI's GPT-4 model, an LLM with 1 trillion parameters, to analyze large amounts of multimodal data, identify patterns and potential risks in a client's technology environment, and, even, predict security breaches and failures. Armed with this insight, Securance tailors its assessment approach to fit each client's organization, address industry concerns, and target technology-specific threats.

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

We Understand Education

The education sector is at high risk for cyber attack because of the breadth and nature of data they store on students and staff, including personally identifiable, healthcare, and financial information. Schools and colleges are also at increased risk because of the size of their attack surfaces, due to the digital capabilities afforded to staff and students via portable devices and the applications used for instruction and tracking, as well as their use of open networks.

Some of the unique challenges the education sector faces include increased attack frequency, limited IT resources, legacy infrastructure, a general lack of cyber awareness, and the need to balance academic openness with cybersecurity. To enable the safe and legally compliant handling of sensitive information, universities like JMU need a cybersecurity partner who understands these challenges, as well as the evolving nature of cybersecurity threats. Securance is that partner, and our experience and expertise prove this.

Securance Experience with Education at a Glance

- **23 years** as a firm serving community college systems, private colleges, major research universities, boards of education, and K–12 school districts.
- Senior cybersecurity consultants, each with **more than 15 years'** experience serving the education sector.
- **50** education and **400** government clients.

Given our qualifications, Securance will bring specific value to JMU, including:

- Experience conducting a variety of IT audits and security assessments for educational institutions and other public entities, including [redacted]
- Familiarity with the needs of public entities in Virginia through several successful partnerships in the state. Besides [redacted]
- Guaranteed responsiveness and continuous communication with JMU's audit department, including on-site work as required, to expedite project completion.
- Familiarity with GLBA, HIPAA, and FERPA requirements and other regulations relevant to JMU.
- Dedication to making findings and recommendations understandable and actionable for all stakeholders.

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

Similar Clients

Below is a sample of clients that have engaged Securance for IT services similar to those sought by JMU.

[redacted]

Case Studies

[redacted]

Case Studies

[redacted]

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

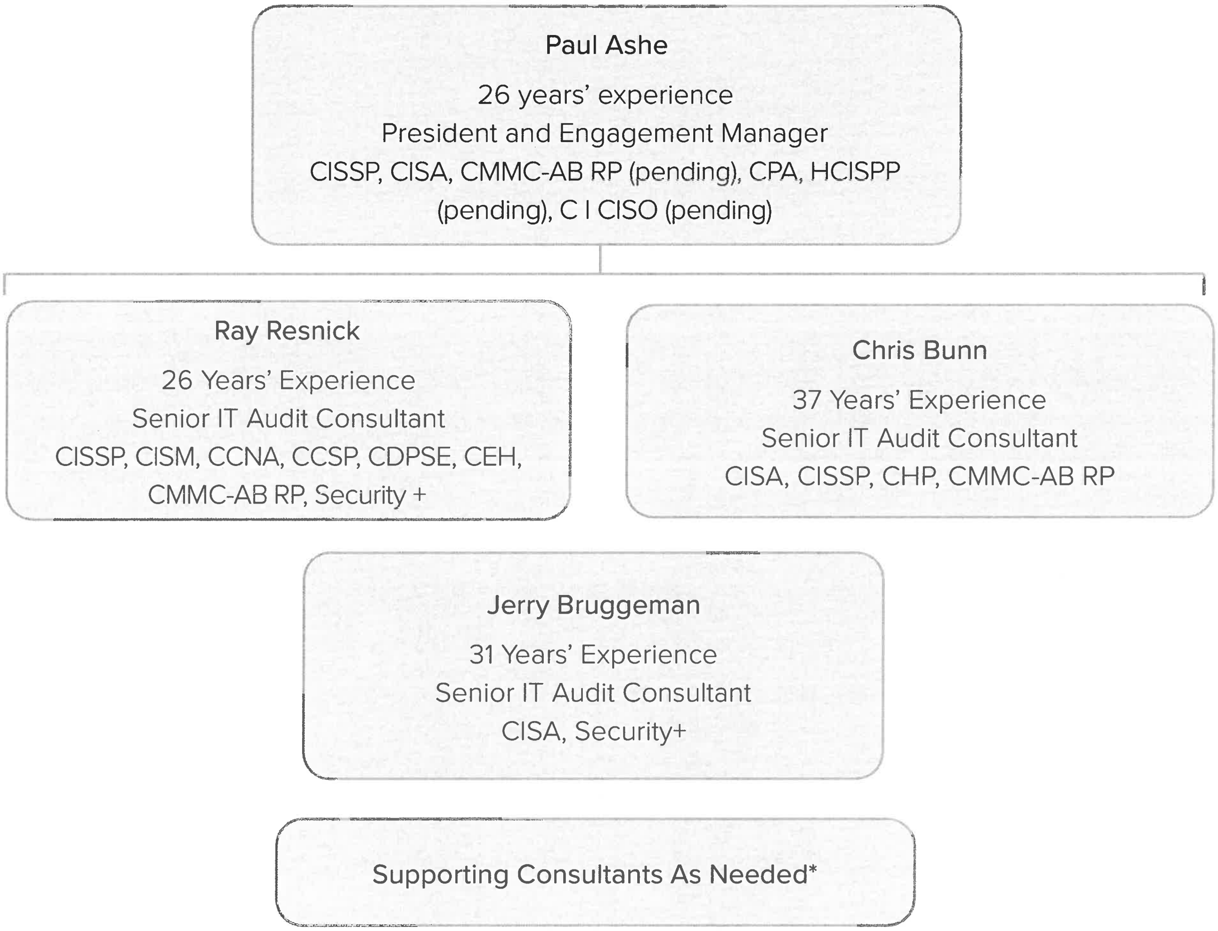
Case Studies

[redacted]

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

Securance's Dedicated Project Team

The expertise and experience of the key personnel listed below align with JMU's definition of "certified professional." If any of these consultants are unavailable when work starts, Securance will propose an equally experienced substitute for approval. All JMU audits will be led by certified professionals.



Paul Ashe
26 years' experience
President and Engagement Manager
CISSP, CISA, CMMC-AB RP (pending), CPA, HCISPP (pending), C I CISO (pending)

Ray Resnick
26 Years' Experience
Senior IT Audit Consultant
CISSP, CISM, CCNA, CCSP, CDPSE, CEH, CMMC-AB RP, Security +

Chris Bunn
37 Years' Experience
Senior IT Audit Consultant
CISA, CISSP, CHP, CMMC-AB RP

Jerry Bruggeman
31 Years' Experience
Senior IT Audit Consultant
CISA, Security+

Supporting Consultants As Needed*

*Securance employs 32 other W2 IT professionals and security consultants that we can leverage to meet JMU's needs. A sample list with a summary of qualifications begins on page 49, and their full resumes will be provided upon request.

Securance's Dedicated Project Team — Key Personnel

PAUL ASHE

27 YEARS OF IT AUDIT EXPERIENCE

President and Engagement Manager | Securance Consulting

EDUCATION

Master of Science
Accounting Information Systems

Bachelor of Science
Accounting and Management Information Systems

PROFESSIONAL CREDENTIALS

- Certified Public Accountant (CPA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Healthcare Information Security and Privacy Practitioner (HCISPP) (pending)
- Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP) (pending)
- Certified Chief Information Security Officer (C | CISO) (pending)

Paul has provided hands-on project management to lead Securance engagements over the past 23 years. A former IT consultant for Ernst & Young, he translates his knowledge and experience into an effective, time- and budget-conscious project management style. Paul conducts IT audits, reviews, and technology-specific vulnerability assessments and penetration tests for clients in nearly every industry and is an expert in implementing and assessing security frameworks.

RELEVANT EXPERIENCE

- Active Directory Reviews
- Cloud Security
- Database Assessments | Data Security
- Endpoint Security
- Enterprise | Web Application Testing
- Firewall | Router Configuration Reviews
- Internal | External | Wireless Network Security
- IT Governance
- Process and Practice Improvement
- Project Management
- Vulnerability Assessments

RELEVANT EXPERTISE

- **Project Management:** Paul has led Securance engagements from kick-off to final report for 23 years.
- **Cyber Resilience:** Paul helps organizations identify threats, risks, and vulnerabilities, and establish full-scale cyber resilience programs to harden their security postures.
- **IT Security Audits:** Paul helps clients identify technical and operational risks and vulnerabilities, develops prioritized remediation recommendations, and guides organizations to focus their resources in the right areas and make informed decisions about IT risk management.
- **Data Security:** Paul is skilled in helping organizations protect the confidentiality, integrity, and availability of their critical data.

Securance's Dedicated Project Team — Key Personnel (continued)

RELEVANT ACHIEVEMENTS

[redacted]

Securance's Dedicated Project Team Key Personnel (continued)

CHRIS BUNN

37 YEARS OF IT AUDIT EXPERIENCE

Senior IT Audit Consultant | Securance Consulting

EDUCATION

Master of Science

Management Information Systems

Bachelor of Science

Computer Science for Business

PROFESSIONAL CREDENTIALS

- Certified Information Systems Security Professional (CISSP)
- Certified HIPAA Professional (CHP)
- Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP)
- Certified Information Systems Auditor (CISA)

Chris is an expert in IT assessments, from best-practice standards to cloud security reviews. His expertise in improving IT processes, evaluating security, assessing and remediating potential threats, and resolving issues caused by internal and external cyber attacks has benefited numerous educational institutions and other government entities.

RELEVANT EXPERIENCE

- Cloud Security
- Data | Information Security
- Federal and State Regulatory Compliance (e.g., GLBA, HIPAA, FERPA)
- IT Audits
- IT Best Practice Deployment (e.g., ISO 27002)
- IT Governance
- Network Device Security Reviews
- Policy and Procedure Development | Review
- Process and Practice Improvement
- Vulnerability Assessments and Penetration Testing
- Web Application Testing

RELEVANT EXPERTISE

- **IT Governance:** Chris is an expert in assessing and developing | implementing IT policies and procedures to ensure efficient operations and compliance with regulatory requirements.
- **IT Best Practice Assessments:** Chris's extensive knowledge of IT security framework standards, including NIST, ISO, COBIT, and ITIL, allows him to provide a holistic assessment across all areas of cyber risk management.
- **Network Security:** Chris excels at identifying and exploiting vulnerabilities in networks, routers, switches, and firewalls and providing actionable remediation recommendations to address each specific vulnerability.

Securance's Dedicated Project Team — Key Personnel (continued)

RELEVANT ACHIEVEMENTS

[redacted]

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

Securance's Dedicated Project Team — Key Personnel (continued)

PRIOR ACHIEVEMENTS

- **East West Bank** | 2012 | Senior Information Security Consultant | Responsible for execution of compliance and risk management projects within the Information Security department of the IT division; developed an IT risk management framework for national and international operations; developed and implemented IT policies and procedures, vendor risk management program, and daily monitoring procedures of critical and high-risk applications and platforms.
- **Experis Finance/Accretive Solution** | 2006–2011 | Senior Risk Advisory Services Consultant | Managed and executed IT audits for various organizations across industries. Audit topics included regulatory compliance, data governance, general computer controls, business continuity, enterprise application controls and security, and process improvement.
- **University of Florida** | 2005–2006 | IT Audit Manager | Planned, supervised, and conducted audits of enterprise applications, data warehouse and reporting systems, financial systems, operations, advisory services, and other projects undertaken by the Office of Audit and Compliance Review; supervised and performed HIPAA compliance audits.
- **BDO Seidman LLP** | 2003–2005 | IT Audit Manager | Member of the BridgeMark risk consulting and advisory services practice; responsible for SAP business intelligence (BI) and governance | risk | compliance advisory services for mySAP ERP with NetWeaver, PeopleSoft, and other service-oriented architecture ERP systems; responsible for project management in technology risk and security, business process improvement, BI and advanced analytics, regulatory compliance, and internal IT audits.
- **Computer Sciences Corporation** | 2000–2003| IT Audit Supervisor | Responsible for the management and execution of service organization (SOC Type II), compliance, internal information system, and pre- and post-implementation audits.
- **Ernst & Young LLP |** 1997–2000 | IT Audit Manager | Member of Information Systems Assurance and Advisory Services (ISAAS) practice; responsible for service organization, general computer controls, IT process reviews, information security engagements, application control consulting, and internal IT audits.
- **Lockheed Martin** | 1994–1997 | IT Audit Supervisor | Performed risk-focused audits of enterprise applications and platforms, system implementations, the enterprise network, engineering online security, and eCommerce security.
- **SunTrust Bank** 1987–1994 | IT Audit Supervisor | Responsible for audits of computer operations, networks, information security policies, enterprise applications, and telecommunications.
- **Blue Cross and Blue Shield of Florida** | 1984–1987 Senior IT Auditor | Supervised reviews of information systems and controls.

Securance's Dedicated Project Team — Key Personnel (continued)

RAY RESNICK

27 YEARS OF IT AUDIT EXPERIENCE

Senior IT Audit Consultant I Securance Consulting

EDUCATION

Bachelor of Science

Accounting

PROFESSIONAL CREDENTIALS

- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate (CCNA)
- CompTIA Security + Certified
- Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP)

Ray, a retired Commander and Special Operations Officer for the U.S. Navy, specializes in analyzing organizational security needs, assessing existing security posture, and implementing plans to mitigate risks to an acceptable level. Ray can work with IT staff at all levels to address risks, vulnerabilities, and gaps that hamper security in the IT environment.

RELEVANT EXPERIENCE

- Active Directory Reviews
- Cloud Security
- Cybersecurity Evaluations
- Database and Operating System Security
- Enterprise and Web Application Security
- Firewall and IDS I IPS Deployment
- Internal I External I Wireless Network Security
- Risk and Threat Analyses
- Server Configuration Reviews
- Voice over Internet Protocol (VoIP) Assessments
- Vulnerability Assessments and Penetration Testing

RELEVANT EXPERTISE

- **IT Risk Assessments:** Ray has been identifying and prioritizing IT security risks for 25 years. His extensive knowledge of IT security framework standards, such as NIST, ISO, COBIT, and ITIL allow him to take a holistic approach across all areas of cyber risk management.
- **Advanced Penetration Testing:** Ray is an experienced ethical hacker, skilled in advanced penetration testing techniques and performing configuration reviews of firewalls and other critical technologies to help organizations protect against potential threats.
- **IT Best Practice Standards:** Ray is well-versed in IT security best practice standards, such as the NIST CSF 2.0, and excels at assessing organizations against those standards and developing gap analyses.

3. EXPERTISE, QUALIFICATIONS, AND EXPERIENCE

Securance's Dedicated Project Team — Key Personnel (continued)

RELEVANT ACHIEVEMENTS

[redacted]

Securance's Dedicated Project Team — Key Personnel (continued)

PRIOR ACHIEVEMENTS

- **Copper Collar Enterprises, LLC** | 2012–2018 | Information Security Engineer | Conducted vulnerability scanning, attack and penetration studies, analyzed information and physical security vulnerability assessments; analyzed data security controls to identify weaknesses; designed remediation strategies.
- **Verizon Communications** | 1998–2003 | Database Administrator | Performed database installs, loads, and data conversions. Tuned and altered databases and tables to increase performance. Prepared custom database reports with SQL and shell scripts. Wrote stored procedures, triggers, and database views to increase efficiency and security. Scheduled and performed database back-ups. Troubleshot application code for SQL errors and potential SQL injection vulnerabilities.
- **Verizon Communications** | 1998–2003 | Senior Systems Engineer | Developed automated tools to improve system reliability and disk and CPU utilization; planned, coordinated, and performed application testing, installation, and patch management; responsible for installing, managing, and administering servers, providing training and technical support to end users, and maintaining system documentation.
- **United States Navy Reserve** | 2002–2003 | Commander | Served as Executive Officer, Operations Department Head (N3), Inspector General, Information Technology and Physical Security Department Head (N6), and Intelligence Department Head (N2); responded to crisis management situations in the United States Central Command Area of Responsibility (USCENTCOM AOR). Supervised Crisis Action Team (CAT cell), Joint Personnel Adjudication System (JPAS), and internal badging systems for U.S. Naval Forces Central Command (NAVCENT); prepared and delivered briefings to Flag Level officers regarding political, military, security, and terrorism matters.
- **United States Navy** | 1991–2007 | Deputy Assistant Chief of Staff Naval Liaison Officer | Performed high-level negotiations with senior governmental officials and military officers from 53 coalition nations; responsible for operational planning efforts of U.S. and coalition maritime assets during wartime environment.

Securance's Dedicated Project Team — Key Personnel (continued)

JERRY BRUGGEMAN

32 YEARS OF IT AUDIT EXPERIENCE

Senior IT Audit Consultant I Securance Consulting

EDUCATION

Bachelor of Science

Cybersecurity

PROFESSIONAL CREDENTIALS

- CompTIA Security + Certified
- Certified Information Systems Auditor (CISA)

Jerry is a versatile cybersecurity expert with a strong background in risk management, networking, IT administration, and IT security. He has helped create and maintain robust information security programs for large organizations in both the private and public sectors, including the U.S. military. Jerry has significant experience conducting internal audits and applying regulatory and best-practice frameworks.

RELEVANT EXPERIENCE

- Active Directory Reviews
- Cybersecurity Assessment
- Database Assessments
- Enterprise and Web Application Security
- Firewall and IDS I IPS Deployment
- IT Audits
- IT Governance
- Network Assessments, e.g., Internal I External I Wireless
- Regulatory and Best-Practice Alignment (e.g., ISO 27002)
- VoIP Assessments
- Vulnerability Assessments and Penetration Testing

RELEVANT EXPERTISE

- **Vulnerability Assessments I Penetration Testing:** Jerry is an ethical hacker with a passion for penetration testing, cyber security, and information security. His exceptional ability to think like a hacker and probe for security vulnerabilities helps organizations enhance their security postures and protect against potential threats.
- **Best Practice Frameworks:** A former director of IT for numerous organizations, public and private, Jerry is an expert in assessing compliance with best practice standards such as ISO, NIST, and COBIT.

Securance's Dedicated Project Team — Key Personnel (continued)

RELEVANT ACHIEVEMENTS WITH SECURANCE

[redacted]

Securance's Dedicated Project Team — Key Personnel (continued)

PRIOR ACHIEVEMENTS

- **HealthPlan Services (Wipro)** | 2020–2023 | Director of Information Security | Provided subject matter expertise in risk assessment, compliance, and technical security.
- **VASTEC** | 2013–2020 | Director of Information Security | Spearheaded IT security program, developed disaster recovery and incident response plans, conducted IT risk assessments, performed and analyzed vulnerability scans, and administered virtual environments.
- **U.S. Air Force, 52nd Combat Communications Squadron** | 2010–2013 | Chief of Cyber Systems Operations | Managed a 120-person team across five work centers, conducted vulnerability and risk assessments, tracked and reported KPIs, and developed and deployed tactical networks.
- **U.S. Air Force, 14th Weather Squadron** | 2005–2010 | Manager, Information Assurance | Managed unit network security programs and assessments; conducted vulnerability and risk assessments.
- **U.S. Air Force Weather Agency** | 2002–2005 | Lead Infrastructure /Information Assurance Technician | Led and trained team responsible for administering and managing the weather network.

As-Needed Personnel

The table below shows the qualifications and experience of Securance team members who can be assigned to JMU engagements as needed. Their full resumes are available upon request.

Name	Title	Education	Certifications	Years of Experience	Relevant Experience
Wajid Hassan	Senior IT Audit Consultant	PhD (in progress) MS BS	CCNA CCNP VCP-550 CCIE AWS CCP	11	Securance, 2024–Present I Senior Cybersecurity Architect Securance for [redacted] 2023–2024 I Senior Cybersecurity Architect, Identity and Access Management TCS Client: Microsoft, 2022 I Network Team Lead TCS Client: Washington Gas Limited, 2022 I Network Team Lead OMM IT Solutions, 2020–2022 I Network Security Architect Amazon Web Services, 2019 I Solutions Architect Seshaat, Inc., 2017–2018 I Network Architect
Jeffrey Kirby	Senior IT Audit Consultant (Incident Response Specialist)	BS	CCNA CIND Security+	17	Securance for [redacted] ls, 2021–Present I Senior Cybersecurity Engineer, Incident Response Department of Veterans Affairs, 2019–2023 I Cyber Hunt and Threat Analyst Smithsonian Institution, 2018–2019 I Cybersecurity Incident Response Manager IRS (contractor), 2017–2018 I Senior Security Engineer Fannie Mae, 2012–2017 I Network Engineer
Montrell Hill	Senior IT Audit Consultant	BS		20	Securance, 2024–Present I Senior IT Audit Consultant First Command Bank I 2019–2022 I Senior IT Auditor I Developed IT audit programs; performed audits and risk assessments; developed strategies to mitigate risks and remediate vulnerabilities. Raytheon, Richardson I 2015–2019 I IT Audit Supervisor and Senior Information Governance & Risk Specialist I Performed IT risk assessments and audits; developed audit programs

As-Needed Personnel

Name	Title	Education	Certifications	Years of Experience	Relevant Experience
Parves Kamal	Senior IT Audit Consultant (Penetration Testing Specialist)	MS BS	CEH Security+ RHCSA RHCE	14	Securance for [redacted] 2019–2020 I Senior Cybersecurity Analyst Synchrony Financial, 2017–2022 I Cybersecurity Senior SOC Analyst Rackspace, 2015–2017 I Senior IT Security Analyst Ameriprise Financials, 2012–2015 I IT Security Analyst Polaris, 2011–2012 I Network Security Consultant
Blas Moreno	Senior IT Audit Consultant	MS BS	CISSP CISSP-ISSAP SSCP AWS CCP Cloud+ CMMC RP	21	Securance for [redacted] 2022 I Senior Cybersecurity Architect Inet-Shield LLC, 2011–2023 I Cybersecurity Architect Prince William County Service Authority, 2017–2020 I Cybersecurity Architect I Analyst American Institutes for Research, 2014–2016 I Lead Cybersecurity Systems Engineer Data Tactics Corporation, 2012–2014 I Data Network Solutions Engineer
Chrystian Torres	Senior IT Security Engineer	MS BS	CCNA CCNP CEH Security+	18	Securance for [redacted] 2021–Present I Senior Cybersecurity Engineer, Vulnerability Management Gray Tier Technologies (contract), 2019–2023 I Red Team Operator, Vulnerability Management Federal Emergency Management Agency (FEMA) (contract), 2016–2019 I Cybersecurity Consultant I Lead Penetration Tester, Vulnerability Management Raytheon, 2017–2019 I Cybersecurity Consultant I Penetration Tester, Vulnerability Management

4. ATTACHMENT A: OFFEROR DATA SHEET

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years 23 Months________

3. REFERENCES: Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact. *Please note that our clients prefer to be contacted first via email.*

CLIENT LENGTH OF SERVICE ADDRESS CONTACT

[redacted]

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

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

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [✓] NO
   IF YES, EXPLAIN:________________________________

5. ATTACHMENT B: SMALL BUSINESS SUBCONTRACTING PLAN

ATTACHMENT B

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: Securance LLC **Preparer Name:** Shawn Johnson

Date: 01.27.2025

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_✓_
If yes, certification number: ____________ Certification date:______________

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_✓_
If yes, certification number: ____________ Certification date:______________

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes____ No_✓_
If yes, certification number: ____________ Certification date:______________

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_✓_
If yes, certification number: ____________ Certification date: ______________

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWAMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of $10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than $3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at http://www.sbsd.virginia.gov/ (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: NA

Date Form Completed: 01.27.2025

Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses
for this Proposal and Subsequent Contract

Offeror / Proposer:

Securance LLC
Firm

13916 Monroes Business Park, Suite 102, Tampa, FL 33635
Address

Shawn Johnson, 817.578.0215 ext. 115
Contact Person/No.

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)
Securance is a minority-owned small business certified in the state of Florida. *We will not employ any subcontractors for this project.*					

(Form shall be submitted with proposal and if awarded, a SWaM Sub-contractor Reporting Form shall be submitted to swamreporting@jmu.edu)

RETURN OF THIS PAGE IS REQUIRED

6. VASCUPP MEMBER SALES

- Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution.

During the past 12 months, Securance has completed projects for one VASCUPP member institution, Radford University. The combined contract value for these projects was $100,795.

(The remainder of this page has been deliberately left blank.)

7. PROPOSED COST

Securance has provided offsite and onsite hourly rates by position in the table below.

Position	Hourly Rate
Offsite Work	
Senior Project Manager	$140
Project Manager	$130
Senior IT Security I Audit Consultant	$145
IT Security I Audit Consultant	$135
Senior IT Security Engineer	$145
Senior Network Engineer	$130
IT Audit Manager	$155
Technical Writer	$75
Onsite Work	
Senior Project Manager	$140
Project Manager	$130
Senior IT Security I Audit Consultant	$145
IT Security I Audit Consultant	$135
Senior IT Security Engineer	$145
Senior Network Engineer	$130
IT Audit Manager	$155
Technical Writer	$75

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

The professional fees listed above are inclusive of all out-of-pocket expenses, and JMU will **NOT** be billed for expenses such as mileage, meals, and incidentals.

7. PROPOSED COST

Hourly Rates

Securance is proposing the hourly rates listed on the previous page, inclusive of labor, travel (if necessary), system licenses, and other reimbursable expenses. The hourly rates apply 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 rates.

Payment Terms

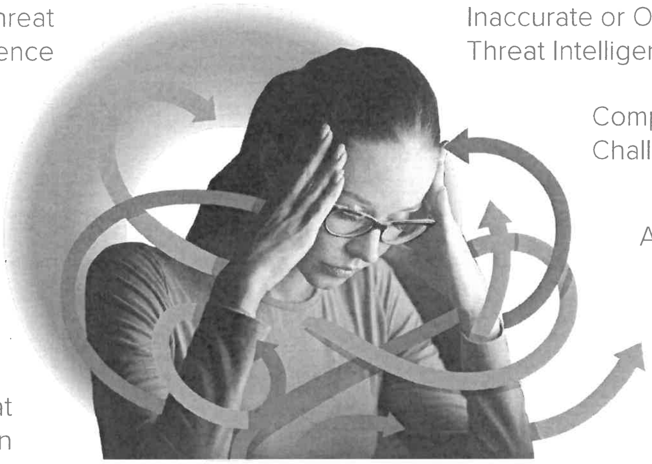
Securance will submit an invoice after delivering a draft management report. All fees are due within 30 days following receipt of invoice. Securance will deliver the final management report following receipt of payment.

If you have questions or would like additional information, do not hesitate to contact us. We want to make sure you have everything you need to make your decision.

We want to partner with you and will be your best partner!

(The remainder of this page has been deliberately left blank.)

THE GROWING CHALLENGE IN CYBERSECURITY



Overload of Threat Intelligence

Incompatibility with Existing Systems

Irrelevance of Generic Threat Information

Resource Strain

Inefficient Threat Prioritization

Inaccurate or Outdated Threat Intelligence

Compliance and Regulatory Challenges

Alert Fatigue

Lack of Actionable Insights

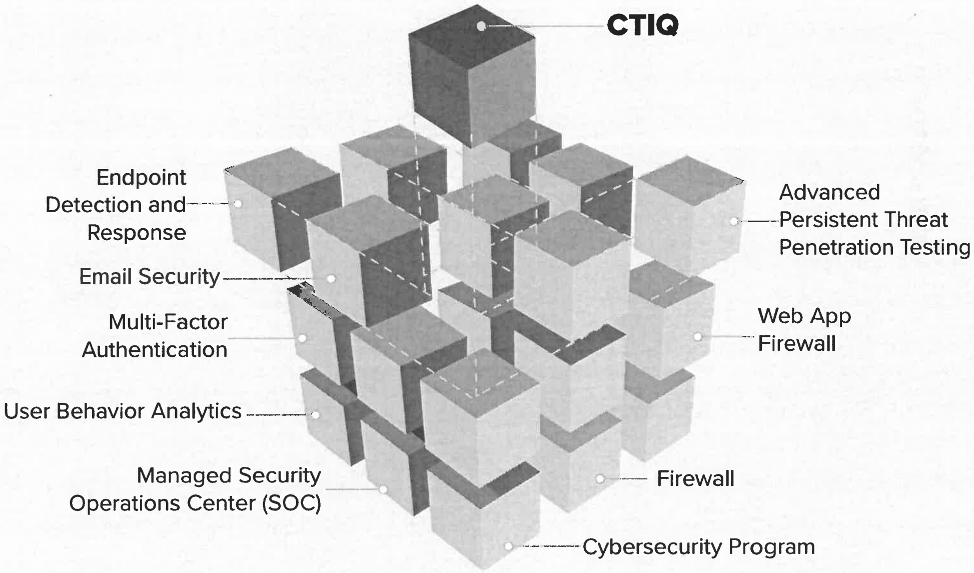
Delayed Response to Threats

REDUCE ALERT FATIGUE

RECEIVE ONLY RELEVANT INFORMATION

PRIORITIZE THREATS

REVOLUTIONIZE YOUR CYBER DEFENSE WITH AI-POWERED INTELLIGENCE



CTIQ

Endpoint Detection and Response

Email Security

Multi-Factor Authentication

User Behavior Analytics

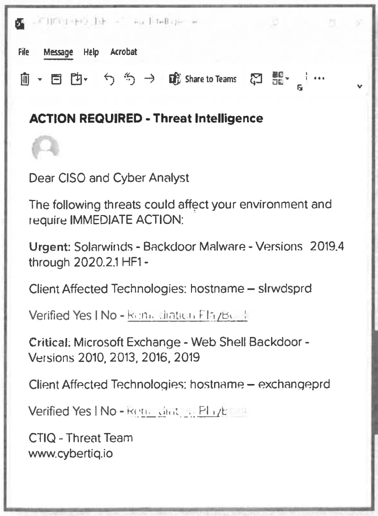
Managed Security Operations Center (SOC)

Advanced Persistent Threat Penetration Testing

Web App Firewall

Firewall

Cybersecurity Program



ACTION REQUIRED - Threat Intelligence

Dear CISO and Cyber Analyst

The following threats could affect your environment and require IMMEDIATE ACTION:

Urgent: Solarwinds - Backdoor Malware - Versions 2019.4 through 2020.2.1 HF1 -

Client Affected Technologies: hostname – slrwdsprd

Verified Yes I No - Remediation PlayBook

Critical: Microsoft Exchange - Web Shell Backdoor - Versions 2010, 2013, 2016, 2019

Client Affected Technologies: hostname – exchangeprd

Verified Yes I No - Remediation PlayBook

CTIQ - Threat Team
www.cybertiq.io

CTIQ utilizes advanced AI technology to gather real-time data from various intelligence sources and centralizes it into one platform. You will receive emails that provide clarity, context, and actionable remediation recommendations specific only to the technology in your environment.

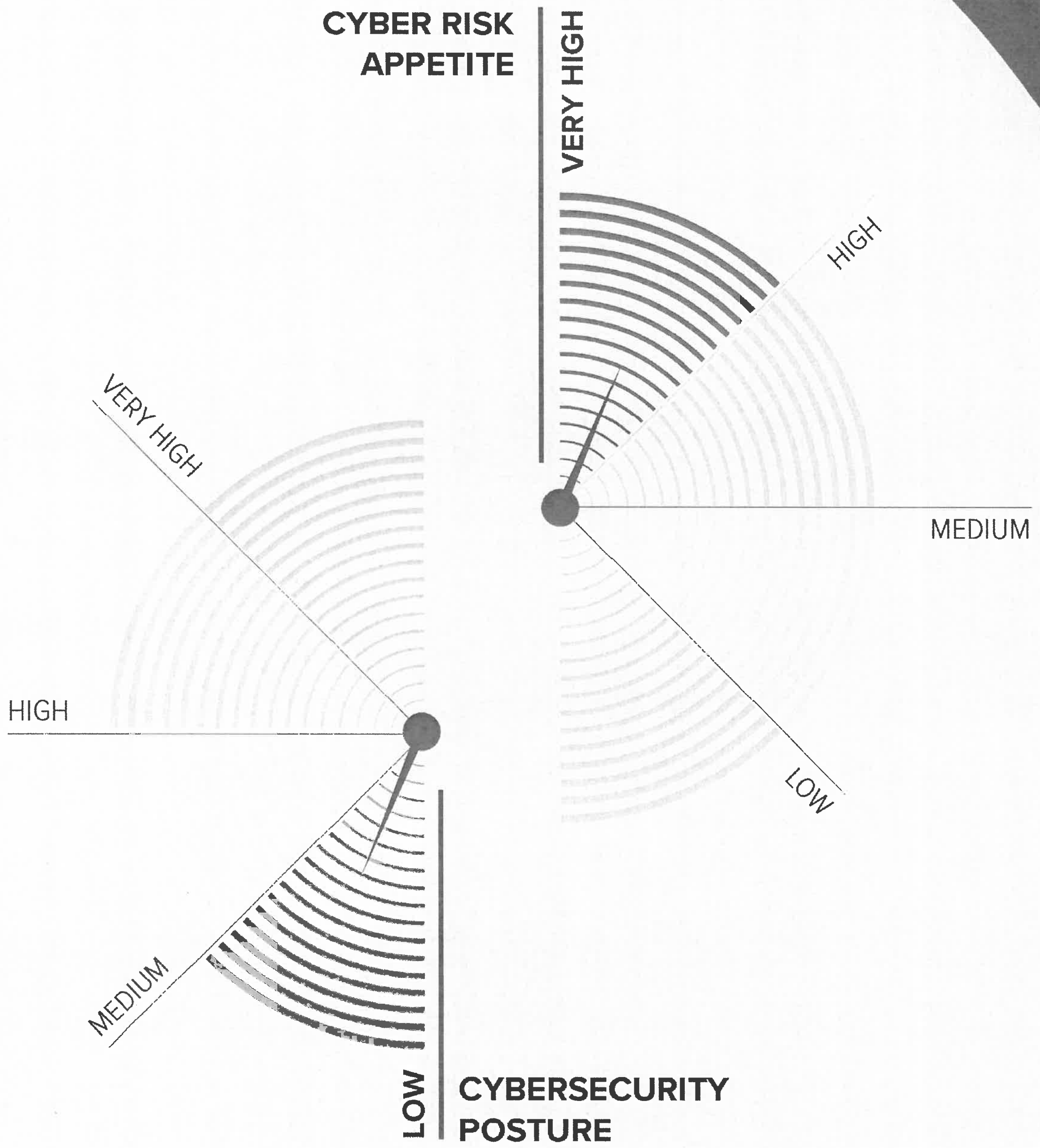
BECOME A BETA CLIENT

https://cybertiq.io/ I info@cybertiq.io

SAMPLE REPORT

SECURANCE CONSULTING

Advantage of Insight AI



IT Security Audit

Date: July 24, 202X

Powered by AI

VERSION MANAGEMENT

Version	Date Approved	Approved By	Brief Description
1.0.0	July 24, 202X	Securance	Initial Report
FINAL		Securance	

This report is intended solely for the management of ABC University for its internal use and is not intended to, nor may, be relied upon by any other party ("Third Party"). Neither this deliverable nor its contents may be distributed to, discussed with, or otherwise disclosed to any Third Party without the prior written permission of Securance Consulting. Securance Consulting accepts no liability or responsibility to any Third Party that gains access to this report.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

Client background information has been redacted. In July 202X, ABC University's (ABC's) IT department contracted Securance to perform a cybersecurity assessment based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF enables organizations, regardless of size, degree of cybersecurity risk, or cybersecurity sophistication, to apply risk management principles and best practices to improve resilience and better manage cybersecurity risks. In addition to the NIST CSF IT risk assessment, the project also included targeted technical vulnerability testing.

Specific Objectives and Scope

The objective of the review was to use the NIST CSF to assess ABC's IT processes and identify vulnerabilities in select technologies. The scope of the review included the following:

- NIST CSF gap analysis using the Core Functions (Identify, Protect, Detect, Respond, and Recover), Categories, and Subcategories
- IT processes:
- Governance policies and procedures – a formal framework of policies and procedures that provides a structure for organizations to ensure that IT investments support business objectives.
- Data and Information Security Management – the prevention of unauthorized access to and use, disruption, modification, and destruction of data assets.
- Indicators of compromise (IoCs) – the process of identifying forensic data, such as that in system log entries or files, that points to potentially malicious activity on a system or network.
- External, internal, heating, ventilation, and air conditioning (HVAC), and closed-circuit television (CCTV) network vulnerability assessment and penetration testing
- Wireless network vulnerability assessment and penetration testing
- Web application vulnerability assessment and penetration testing
- Network firewall configuration assessment
- IoC testing

Approach and Methodology

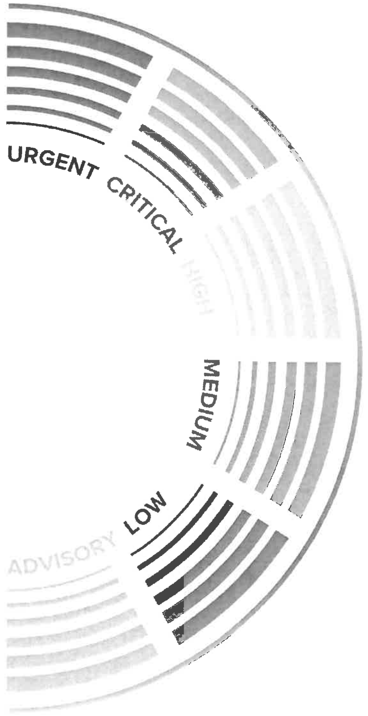
We based our approach on our proven methodologies to ensure a comprehensive assessment. This approach included the following activities:

- Review of IT policies, procedures, and standards.
- Interviews with IT management and personnel.
- Review of collected evidence and testing of relevant IT operations and processes; and
- Use of commercial security tools and manual testing techniques.

The review was limited to the areas we considered necessary to complete the assessment and was not intended to cover ABC's entire information systems function.

The remainder of page left blank intentionally.

Finding Legend:



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

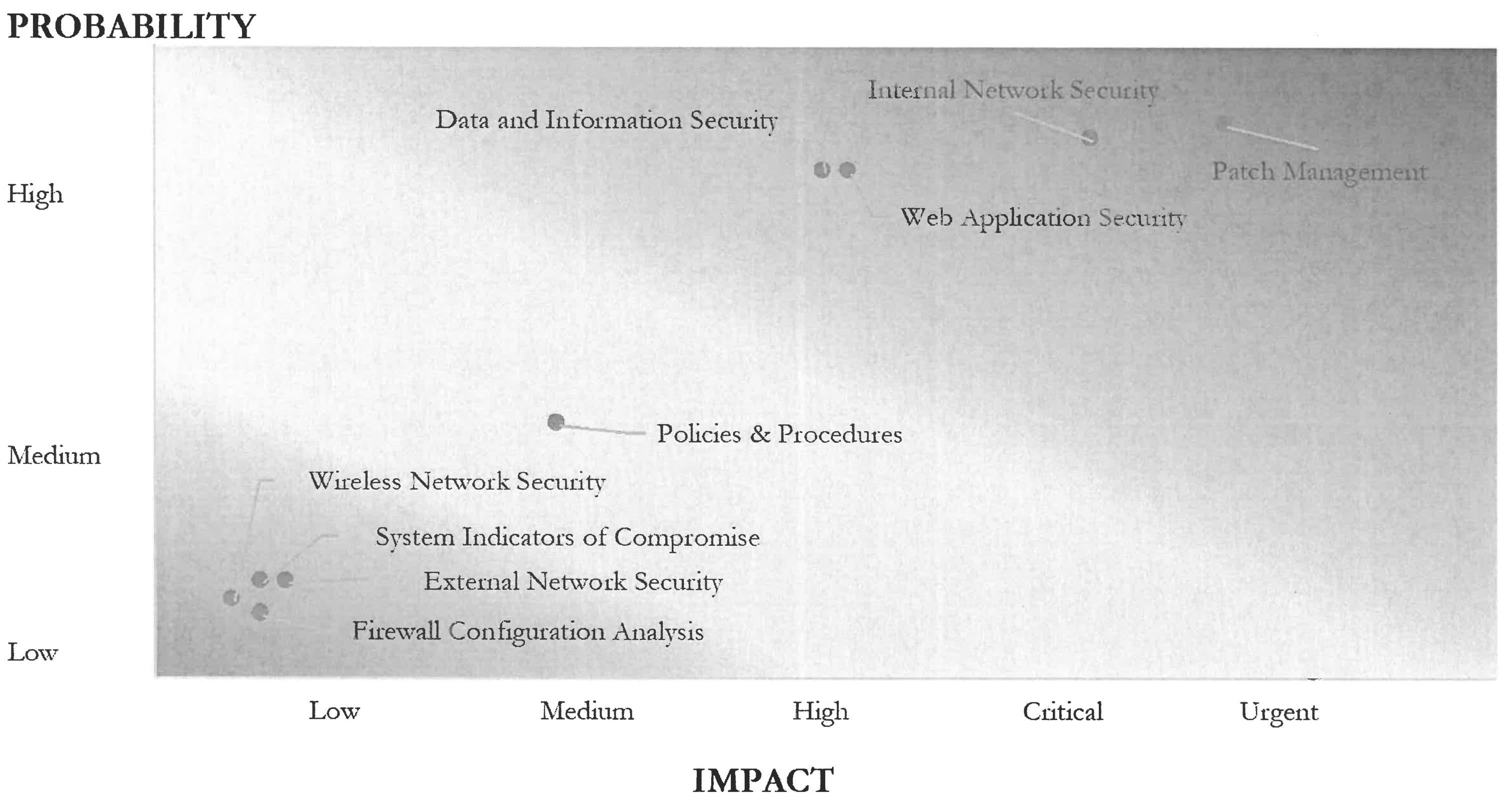
Summary of Findings – ABC University

The following section provides a summary of our findings from the cybersecurity assessment.

No.	Finding Title	5	4	3	2	1	0
1	Patch Management	✓					
2	Internal Network Vulnerability Assessment and Penetration		✓				
3	Data and Information Security			✓			
4	Web Application Vulnerability Assessment			✓			
5	Policies and Procedures				✓		
6	Firewall Configuration Analysis					✓	
7	Wireless Network Assessment					✓	
8	External Network Vulnerability Assessment					✓	
9	System IoCs					✓	
10	Firewall Optimization						✓
11	Website and Web Application Housekeeping						✓
12	External Network Public Information						✓
	Total Findings:	1	1	2	1	4	3

The remainder of page left blank intentionally.

CYBERSECURITY ASSESSMENT HEAT MAP



5 **No. 1: Patch Management** – we evaluated the patch management process by scanning the internal network using Nessus Professional. The results of our scans indicate that the patch management process should be improved.

4 **No. 2: Internal Network Vulnerability Assessment and Penetration Test** – we scanned ABC's internal network and identified 25 critical-, 23 high-, and 45 medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach. In addition, we successfully exploited vulnerabilities on several hosts.

3 **No. 3: Data and Information Security** – the objective of a data and information security program is to prevent unauthorized access to and use, disruption, modification, and destruction of data assets. Securance identified several opportunities to improve the security of ABC's data assets.

3 **No 4: Web Application Vulnerability Assessment** – we performed a detailed security assessment of several Internet-facing web applications and identified technical vulnerabilities that ABC should remediate.

2 **No 5: Policies and Procedures** – we reviewed several IT policies and governance documents and recommend slight modifications to them. In addition, we recommend that ABC develop a playbook to support the incident response plan (IRP), implement a cybersecurity resilience program (CRP), and perform annual tabletop exercises.

Conclusion

Based on our assessment, knowledge of ABC's computing environment, and IT security experience, we identified several opportunities to improve ABC's IT security controls and reduce cyber risks to an acceptable level.

We recommend that ABC review and implement our recommendations to improve its cybersecurity posture and process controls. The remainder of this report provides an analysis of our approach and methodology, the risks we identified, and detailed mitigation recommendations.

IT SECURITY AUDIT REPORT

Background

Client background information has been redacted.

In July 2023, ABC's IT department contracted Securance to perform a cybersecurity assessment based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF enables organizations, regardless of size, degree of cybersecurity risk, or cybersecurity sophistication, to apply risk management principles and best practices to improve resilience and better manage cybersecurity risks. In addition to the NIST CSF IT risk assessment, the project also included targeted technical vulnerability testing.

Specific Objectives and Scope

The objective of the review was to use the NIST CSF to assess ABC's IT processes and identify vulnerabilities in select technologies. The scope of the review included the following:

1. IT processes and procedures associated with the following NIST CSF domains:
    - Identify – an organization's ability to fully understand its current IT environment so it can successfully manage emerging cybersecurity threats affecting data, systems, and assets. Categories include Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Plan, and Supply Chain Risk.
    - Protect – an organization's ability to provide sufficient protection to ensure delivery of services. Categories include Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Procedures and Processes, Maintenance, and Protective Technology.
    - Detect – an organization's ability to identify cybersecurity events. Categories include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.
    - Respond – an organization's ability to contain the adverse effects of a cybersecurity event. Categories include Response Planning, Communications, Analysis, Mitigation, and Improvements.
    - Recover – an organization's ability to achieve business resilience. Categories include Recovery Planning, Improvements, and Communications.

2. IT processes:
   - Governance policies and procedures – a formal framework of policies and procedures that provides a structure for organizations to ensure that IT investments support business objectives.
   - Data and Information Security Management – the prevention of unauthorized access to and use, disruption, modification, and destruction of data assets.
   - Indicators of compromise (IoCs) – the process of identifying forensic data, such as that in system log entries or files, that points to potentially malicious activity on a system or network.

3. External network subnet XX.XXX.XXX.X/XX.

4. Internal network subnets:
   - XX.XX.X.X/XX
   - XX.XX.XX.X/XX
   - XX.XX.XX.X/XX
   - XX.XX.XX.X/XX
   - XX.XX.XX.X/XX
   - XX.XX.X.X/XX
   - XX.XX.X.X/XX
     XX.XX.X.X/XX

5. Wireless network – Juniper Mist

6. Internet-facing web applications:
   - ABC Employee Contracts – https://www.xxxxx-x1.net
   - Safety Video Viewing/Tracking – https://www.xxxxx-x2.net
   - SIS Training Registration – https://www.xxxxx-x3.net
   - Admin Office Front Desk Sign-In – https://www.xxxxx-x4.net
   - Incident Reporting – https://www.xxxxx-x5.net
   - Retirement Counseling Registration – https://www.xxxxx-x6.net
   - Contact Forms – https://www.xxxxx-x7.net
   - Hotspot Request Form – https://www.xxxxx-x8.net
   - Web Request Form – https://www.xxxxx-x9.net
   - Student Information System – https://www.xxxxx-x10.net

7. Analyses of ABC's firewalls:
    - CheckPoint 23800 Security Gateway (OS: R81.10)
    - Fortigate-1
    - Fortigate-2
    - Fortigate-3
    - Fortigate-4
    - Fortigate-5

8. Indicators of compromise (IoC) testing on the following hosts:
    - Domain controller (hostname: SSC-DC01 | XX.XX.XX.XX)
    - Database server (hostname: SSC-FS1 | XX.XX.XX.X)
    - File server (hostname: SQL | XX.XX.X.XX)

Approach and Methodology

To achieve ABC's objectives, we relied on our proven assessment methodologies, summarized below:

NIST CSF AND IT PROCESS RISK ASSESSMENTS

During these phases, our procedures included:

- Review of IT policies, procedures, and standards.
- Interviews with ABC's IT process owners.
- Review of supporting assessment evidence and artifacts.
- Analysis of system and network event logs for forensic evidence.

EXTERNAL, INTERNAL, HVAC, AND CCTV NETWORK TESTING

We used discovery, vulnerability assessment, and penetration testing procedures, listed below, to identify weaknesses in IP network services:

- Internet Discovery – using public tools, manual tasks, publicly available information, and information from ABC's IT management, we created a profile of computer addresses and other information about ABC's external, internal, heating, ventilation, and air conditioning (HVAC), and closed-circuit television (CCTV) networks.
- External, Internal, HVAC, and CCTV Network IP Scans – using Nmap and Nessus Professional vulnerability scanner, we scanned the approved ranges of IP addresses. We configured scanning policies that minimized disruption to ABC's network systems and devices. This included disabling denial of service and brute force attack attempts.
- False Positive Identification – we analyzed the results and, based on our knowledge and information from the scans, attempted to identify and remove all false-positive vulnerabilities.
- Penetration Testing – we attempted to exploit select vulnerabilities on the internal network and gain access to system resources.

WIRELESS NETWORK TESTING

We used commercial wireless system scanners, including KisMAC and Air Magnet, to assess the wireless network. Our procedures included, but were not limited to, the following:

- Wireless Discovery – we created a profile of available wireless networks and determined each network's service set identifier (SSID) and level of encryption.
- Architectural Assessment – we gained an understanding of the wireless architecture and the process of administering the wireless network.
- Attempted to Gain Access – after identifying the wireless networks, we tried to access each one by obtaining a username and password from a connected user without his knowledge.

WEB APPLICATION ASSESSMENT

Using Nmap, a commercial port scanner, and nStalker, a commercial web-application security testing tool, we tested each web application for vulnerabilities in the following categories:

- Cross-Site Scripting
- SQL Injection
- Remote Execution
- Directory/File Traversal
- CRLF Injection
- PHP File Include
- Parameter Deletion
- Special Parameter Addition
- Boolean Parameter Tampering
- Blind SQL Injection
- Buffer Overflow
- Format String
- Integer Overflow
- Information Exposure
- Generic HTTP Attacks
- Microsoft CGI Attacks
- CGI Attacks
- Microsoft IIS Attacks
- Common HTTP Device Attacks

FIREWALLS

We used Firewall Analyzer and Nipper Studio to analyze each firewall's configuration file, line by line.

The review was limited to the areas we considered necessary to complete the assessment and was not intended to cover ABC's entire information systems function.

Remainder of page left blank intentionally.

NIST CSF ANALYSIS – FRAMEWORK CORE

Function	Category	Subcategory	Tier	Comment
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	2 – Risk-Informed	ABC uses Freshworks Freshservice IT service management (ITSM) and One to One Plus K–12 asset management/helpdesk software to record IT hardware and software assets. Post-Remediation: ↑3 – Repeatable
		ID.AM-2: Software platforms and applications within the organization are inventoried.	2 – Risk-Informed	
		ID.AM-3: Organizational communication and data flows are mapped.	1 – Partial	Document data assets and flows. Post-Remediation: ↑2 – Risk-Informed
		ID.AM-4: External information systems are catalogued.	2 – Risk-Informed	Refer to ID.AM-2. Post-Remediation: ↑3 – Repeatable
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	2 – Risk-Informed	Update asset inventory to include asset classification, criticality, and business value. Post-Remediation: ↑3 – Repeatable
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	2 – Risk-Informed	Ensure IRP includes defined roles and responsibilities for cybersecurity team, including chain of command. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated.	1 – Partial	Not yet documented. Document in the Risk Management Procedure. Post-Remediation: ↑2 – Risk-Informed
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.	2 – Risk-Informed	Continue to mature the cybersecurity posture and integrate critical third parties. Post-Remediation: ↑3 – Repeatable
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	1 – Partial	Develop an IT strategic plan mapped to ABC' strategic plan. Post-Remediation: ↑2 – Risk-Informed
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	2 – Risk-Informed	Annually test the disaster recovery plan (DRP) and incident response plan (IRP) via system recovery and tabletop exercises, respectively. Post-Remediation: ↑3 – Repeatable
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	2 – Risk-Informed	

*A comprehensive cybersecurity program should include the following components to align with the NIST CSF:

IDENTIFY

- Threat intelligence (TI) process
- Threat actor matrix
- Analysis of TI relative to NPPS's technology environment
- Monitoring of IT assets – security operations center (SOC)
- Annual IT risk assessments
- Incorporation of IT risk landscape into overall risk
- management strategy

PROTECT

- Strong network access controls
- Multi-factor authentication (MFA)
- Effective user provisioning
- End-user training
- Data security
- IT governance
- Patch management
- Vulnerability management
- Vendor risk management
- Strong contractual language
- Intrusion protection system (IPS)
- Domain nameserver management
- Endpoint security
- Periodic user reviews
- Chief information security officer
- Participation in security conferences regarding current protect techniques, tactics, and practices

DETECT

- 24x7x365 SOC
- Employee training in reporting of anomalies and events
- Intrusion detection system (IDS)
- Effective endpoint security, including an endpoint detection and response solution.
- Participation in security conferences to learn new detect techniques, tactics, and practices

RESPOND

- IRP
- Incident escalation process
- Annual tabletop exercises
- Lessons learned analyses and updates to the IRP

RECOVER

- DRP
- Annual testing of the DRP – rotating technologies
- Lessons learned analyses and updates the DRP – annually and as needed

Function	Category	Subcategory	Tier	Comment
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	2 – Risk-Informed	Cybersecurity policy references vulnerability scanning. However, limited evidence of a formal vulnerability management program. Post-Remediation: ↑3 – Repeatable
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	2 – Risk-Informed	ABC receives TI but does not map it to the current technology profile. Post-Remediation: ↑3 – Risk-Informed
		ID.RA-3: Threats, both internal and external, are identified and documented.	2 – Risk-Informed	
		ID.RA-4: Potential business impacts and likelihoods are identified.	2 – Risk-Informed	DRP and IRP exist. Annually test the DRP and IRP via system recovery and tabletop exercises, respectively. Post-Remediation: ↑3 – Repeatable
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	2 – Risk-Informed	
		ID.RA-6: Risk responses are identified and prioritized.	2 – Risk-Informed	

Function	Category	Subcategory	Tier	Comment
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	2 – Risk-Informed	Risk management procedure exists, but there is limited evidence of implementation. Post-Remediation: ↑2 – Repeatable
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	1 – Partial	Define risk tolerance by establishing current cybersecurity posture. Post-Remediation: ↑2 – Risk-Informed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.	1 – Partial	

Remainder of page left blank intentionally.

Function	Category	Subcategory	Tier	Comment
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	1 – Partial	Supply chain risk not incorporated in risk management procedure. Post-Remediation: ↑2 – Risk-Informed
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	1 – Partial	Implement a formal, repeatable vendor risk assessment process. Post-Remediation: ↑2 – Risk-Informed
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	1 – Partial	Modify contracts with suppliers to incorporate cyber risk measures consistent with ABC standards. Post-Remediation: ↑2 – Risk-Informed
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	1 – Partial	Periodically review vendors' compliance with ABC standards. Post-Remediation: ↑2 – Risk-Informed
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	2 – Risk-Informed	DRP and IRP exist. Annually test the DRP and IRP via system recovery and tabletop exercises, respectively. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	2 – Risk-Informed	Automated process in place for adding, changing, and removing Active Directory accounts in the production environment. Perform periodic user reviews. Post-Remediation: ↑3 – Repeatable
		PR.AC-2: Physical access to assets is managed and protected.	2 – Risk-Informed	Data center (DC) uses Lenel access control and physical keys for security. Improve physical security of all physical locations. Post-Remediation: ↑3 – Repeatable
		PR.AC-3: Remote access is managed.	2 – Risk-Informed	Virtual private network (VPN) and MFA required. Post-Remediation: ↑3 – Repeatable
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	2 – Risk-Informed	Refer to PR.AC-1. Post-Remediation: ↑3 – Repeatable
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	2 – Risk-Informed	Network segregation/segmentation implemented physically and via virtual local area networks (VLANs). Add access control lists (ACLs) to improve restrictions. Post-Remediation: ↑3 – Repeatable
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	2 – Risk-Informed	Refer to PR.AC-1. Post-Remediation: ↑3 – Repeatable
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	2 – Risk-Informed	Refer to PR.AC-1. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained.	2 – Risk-Informed	A cybersecurity training and awareness policy exists, and introductory training is provided. However, no formal training program is in place. Post-Remediation: ↑3 – Repeatable
		PR.AT-2: Privileged users understand their roles and responsibilities.	2 – Risk-Informed	Privileged IT and application users informally understand their roles. However, roles should be documented in a formal cybersecurity policy or program and reviewed annually. Post-Remediation: ↑3 – Repeatable
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	1 – Partial	Implement a formal, repeatable vendor risk assessment process. Post-Remediation: ↑2 – Risk-Informed
		PR.AT-4: Senior executives understand their roles and responsibilities.	2 – Risk-Informed	Ensure IRP includes defined roles and responsibilities for cybersecurity team, including chain of command. Post-Remediation: ↑3 – Repeatable
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	2 – Risk-Informed	

Function	Category	Subcategory	Tier	Comment
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected.	1 – Partial	Data is not encrypted at rest. Encrypt sensitive data. Post-Remediation: ↑2 – Risk-Informed
		PR.DS-2: Data-in-transit is protected.	2 – Risk-Informed	Web application data is encrypted in transit. Ensure on-premise application data is encrypted. Post-Remediation: ↑3 – Repeatable
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	2 – Risk-Informed	Assets appear adequately tracked. However, formal destruction policy not in place. Post-Remediation: ↑3 – Repeatable
		PR.DS-4: Adequate capacity to ensure availability is maintained.	1 – Partial	System capacity managed informally. Post-Remediation: ↑2 – Risk-Informed
		PR.DS-5: Protections against data leaks are implemented.	1 – Partial	Implement data loss prevention (DLP) solution. Post-Remediation: ↑2 – Risk-Informed
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	1 – Partial	Evidence of integrity checking not available. Post-Remediation: ↑2 – Risk-Informed
		PR.DS-7: The development and testing environment(s) are separate from the production environment.	2 – Risk-Informed	Separation of development and testing environments appears appropriate to support ABC operations. Continue to review separation of environments. Post-Remediation: ↑3 – Repeatable
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	1 – Partial	Refer to PR.DS-6. Post-Remediation: ↑2 – Risk-Informed

Function	Category	Subcategory	Tier	Comment
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).	1 – Partial	Configuration baselines not in place. Adopt Center for Internet Security (CIS) baseline standards. Post-Remediation: ↑2 – Risk-Informed
		PR.IP-2: A System Development Life Cycle to manage systems is implemented.	1 – Partial	Draft and implement a formal system development life cycle (SDLC) and supporting documents. Post-Remediation: ↑2 – Risk-Informed
		PR.IP-3: Configuration change control processes are in place.	1 – Partial	Refer to PR.IP-1. Post-Remediation: ↑2 – Risk-Informed
		PR.IP-4: Backups of information are conducted, maintained, and tested.	3 – Repeatable	Backup process operates effectively. Perform full system recovery test annually. Post-Remediation: ↑4 – Adaptive
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	2 – Risk-Informed	DC uses Lenel access control and physical keys for security. Improve physical security of all physical locations. Post-Remediation: ↑3 – Repeatable
		PR.IP-6: Data is destroyed according to policy.	2 – Risk-Informed	Assets appear adequately tracked. However, formal destruction policy not in place. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP) (continued):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-7**: Protection processes are improved.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable
		PR.IP-8: Effectiveness of protection technologies is shared.	2 – Risk-Informed	
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	2 – Risk-Informed	DRP and IRP exist. Annually test the DRP and IRP via system recovery and tabletop exercises, respectively. Post-Remediation: ↑3 – Repeatable
		PR.IP-10: Response and recovery plans are tested.	2 – Risk-Informed	
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	2 – Risk-Informed	A cybersecurity training and awareness policy exists, and introductory training is provided. However, no formal training program is in place. Post-Remediation: ↑3 – Repeatable
		PR.IP-12: A vulnerability management plan is developed and implemented.	2 – Risk-Informed	Cybersecurity policy references vulnerability scanning. However, limited evidence of a formal vulnerability management program. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	2 – Risk-Informed	Formalize the change management policy and procedure to capture all changes to the environment. Post-Remediation: ↑3 – Repeatable
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	2 – Risk-Informed	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	2 – Risk-Informed	Adequate logging and audit records exist and are managed. Post-Remediation: ↑3 – Repeatable
		PR.PT-2: Removable media is protected, and its use restricted according to policy.	1 – Partial	Removable media is not tracked or inventoried. Implement a method to track removable media. Post-Remediation: ↑2 – Risk-Informed
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	2 – Risk-Informed	Automated process in place for adding, changing, and removing Active Directory accounts in the production environment. Perform periodic user reviews. Post-Remediation: ↑3 – Repeatable
		PR.PT-4: Communications and control networks are protected.	2 – Risk-Informed	Refer to DE.AE-2 – DE.AE-5. Post-Remediation: ↑3 – Repeatable
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	1 – Partial	System capacity managed informally. Post-Remediation: ↑2 – Risk-Informed

Function	Category	Subcategory	Tier	Comment
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	2 – Risk-Informed	Document normal network data flows and user behavior. Post-Remediation: ↑3 – Repeatable
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	2 – Risk-Informed	ABC uses Splunk Cloud for IT infrastructure monitoring (e.g., firewalls, domain controllers, and servers). Splunk does not monitor entire production environment. Uses Paessler PRTG for network monitoring and ExtraHop, a cloud-native network detection and response solution, to monitor network traffic. Local logging is enabled on servers, workstations, and laptops. Email alerts are sent to applicable IT personnel. Continue to tune and improve monitoring processes. Post-Remediation: ↑3 – Repeatable
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	2 – Risk-Informed	
		DE.AE-4: Impact of events is determined.	2 – Risk-Informed	
		DE.AE-5: Incident alert thresholds are established.	2 – Risk-Informed	

Function	Category	Subcategory	Tier	Comment
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	2 – Risk-Informed	Refer to DE.AE-2 – DE.AE-5. Post-Remediation: ↑3 – Repeatable
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	2 – Risk-Informed	DC uses Lenel access control and physical keys for security. Cameras in place at DC and throughout the organization. Improve physical security of all physical locations. Post-Remediation: ↑3 – Repeatable
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	2 – Risk-Informed	Document normal network data flows and user behavior. Post-Remediation: ↑3 – Repeatable
		DE.CM-4: Malicious code is detected.	2 – Risk-Informed	Refer to DE.AE-2 – DE.AE-5. Post-Remediation: ↑3 – Repeatable
		DE.CM-5: Unauthorized mobile code is detected.	2 – Risk-Informed	
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	1 – Partial	No evidence of monitoring external service providers. Implement a formal vendor risk management program. Post-Remediation: ↑2 – Risk Informed
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	2 – Risk-Informed	Refer to DE.AE-2 – DE.AE-5. Post-Remediation: ↑3 – Repeatable
		DE.CM-8: Vulnerability scans are performed.	2 – Risk-Informed	Cybersecurity policy references vulnerability scanning. However, limited evidence of a formal vulnerability management program. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability.	2 – Risk-Informed	Ensure IRP includes defined roles and responsibilities for cybersecurity team, including chain of command. Post-Remediation: ↑3 – Repeatable
		DE.DP-2: Detection activities comply with all applicable requirements.	2 – Risk-Informed	Continuously monitor compliance requirements. Post-Remediation: ↑3 – Repeatable
		DE.DP-3: Detection processes are tested.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable
		DE.DP-4: Event detection information is communicated.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable
		DE.DP-5: Detection processes are continuously improved.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed.	2 – Risk-Informed	
		RS.CO-2: Incidents are reported consistent with established criteria.	2 – Risk-Informed	
		RS.CO-3: Information is shared consistent with response plans.	2 – Risk-Informed	
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	2 – Risk-Informed	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	2 – Risk-Informed	

Function	Category	Subcategory	Tier	Comment
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated.	2 – Risk-Informed	Use of multiple tools. Continue to improve this process. Post-Remediation: ↑3 – Repeatable
		RS.AN-2: The impact of the incident is understood.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable
		RS.AN-3: Forensics are performed.	2 – Risk-Informed	
		RS.AN-4: Incidents are categorized consistent with response plans.	2 – Risk-Informed	
		RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	2 – Risk-Informed	Use of multiple tools. Continue to improve this process. Post-Remediation: ↑3 – Repeatable
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3– Repeatable
		RS.MI-2: Incidents are mitigated.	2 – Risk-Informed	
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	2 – Risk-Informed	Use of multiple tools. Continue to improve this process. Post-Remediation: ↑3 – Repeatable

Function	Category	Subcategory	Tier	Comment
RESPOND (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned.	2 – Risk-Informed	IRP exists. Perform annual tabletop testing and update the IRP based on testing results. Post-Remediation: ↑3 – Repeatable
		RS.IM-2: Response strategies are updated.	2 – Risk-Informed	

Remainder of page left blank intentionally.

Function	Category	Subcategory	Tier	Comment
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident.	2 – Risk-Informed	DRP and IRP exist. Annually test the DRP and IRP via system recovery and tabletop exercises, respectively. Post-Remediation: ↑3 – Repeatable
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned.	2 – Risk-Informed	
		RC.IM-2: Recovery strategies are updated.	2 – Risk-Informed	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed.	2 – Risk-Informed	
		RC.CO-2: Reputation is repaired after an incident.	2 – Risk-Informed	
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	2 – Risk-Informed	

NIST CSF ANALYSIS – FRAMEWORK IMPLEMENTATION TIERS

The Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business or mission objectives, supply chain cybersecurity requirements, and organizational constraints. The Tiers are summarized below:

Tier 1: Partial

- Risk Management Process – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc, and sometimes reactive, manner.

- Integrated Risk Management Program – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis, due to varied experience or information gained from outside sources.

- External Participation – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, or information about technologies) from other entities, nor does it share information.

Tier 2: Risk-Informed

- Risk Management Process – Risk management practices are approved by management but may not be established as organization-wide policy.

- Integrated Risk Management Program – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.

- External Participation – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information but may not share information with others.

Tier 3: Repeatable

- Risk Management Process – The organization's risk management practices are formally approved and expressed as policy.

- Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. The organization consistently and accurately monitors cybersecurity risk to organizational assets.

- External Participation – The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It regularly collaborates with and receives information from other entities to complement internally generated information, and shares information with other entities.

Tier 4: Adaptive

- Risk Management Process – The organization adapts its cybersecurity practices based on past and current cybersecurity activities, including lessons learned and predictive indicators.

- Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Senior executives monitor cybersecurity risk in the same context as financial and other organizational risks. Business units implement the executive vision and analyze system-level risks in the context of organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of prior activities and continuous monitoring of systems and networks.

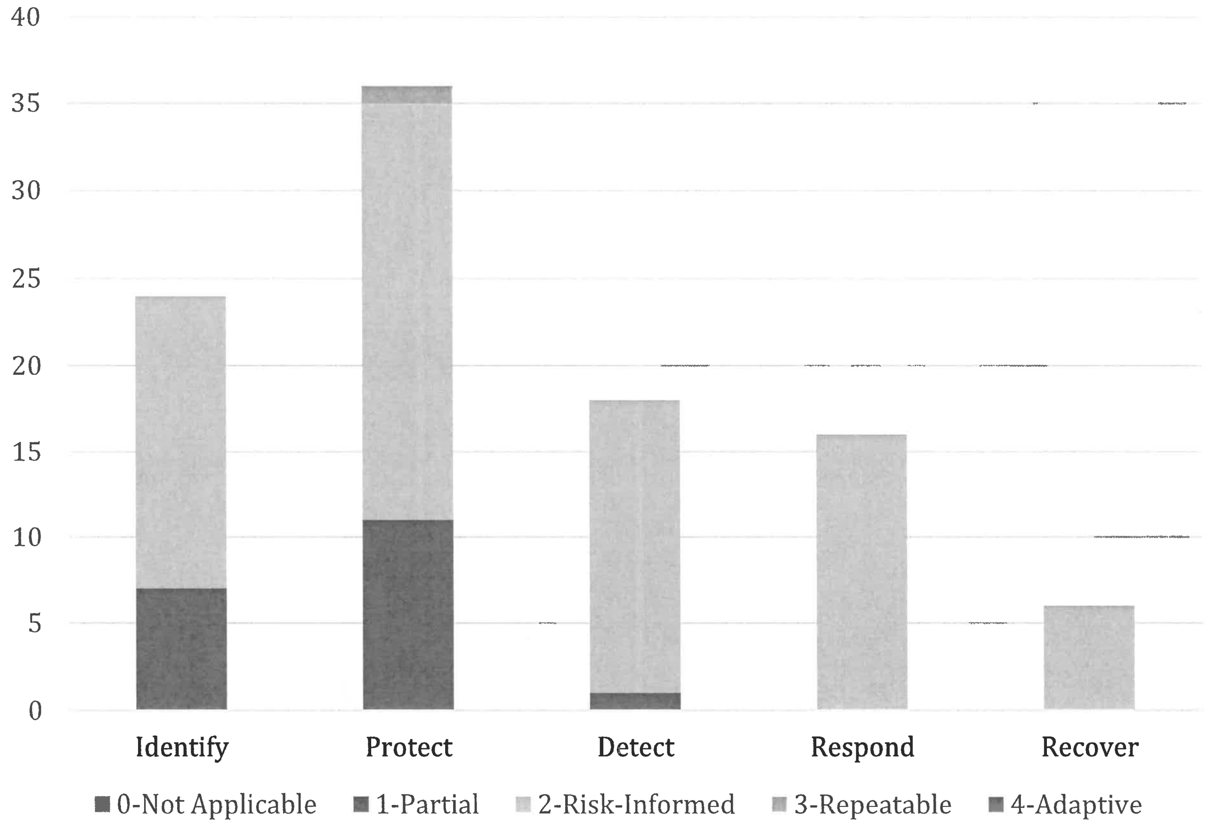
- External Participation – The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or a higher Tier, the Tiers do not represent maturity levels. The Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and require additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

Remainder of page left blank intentionally.

NIST CSF ANALYSIS – FRAMEWORK PROFILE

An organization's Profile is the alignment of the Functions, Categories, and Subcategories with its business requirements, risk tolerance, and resources. Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities within the organization. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. The bar chart below depicts ABC's current Tier for each Function, Category, and Subcategory.



ABC's Current Profile is based on the Category and Subcategory outcomes from the Framework Core that are currently being achieved. Based on our assessment and our IT risk assessment experience, ABC's current state spans two Tiers, Tier 1, Partial, and Tier 2, Risk Informed.

ABC's major deficiencies include the absence of the following:

Formal IT governance documents, including an IT strategic plan mapped to the organization's strategic plan, an IT risk assessment program, data flow diagrams, and disaster recovery and incident response plan annual testing strategies.

A data management and ownership program, including data classification and protection.

A comprehensive cybersecurity program, with supporting technologies and human resources.

ABC should continue working to improve its Current Profile. Improvement is achieved by allocating the necessary resources to remediate observations in IT risk assessment reports and by continuing processes currently deemed effective. Reaching the Adaptive Tier requires an environment where management and staff continually implement improvements based on lessons learned and work to create a cyber-aware culture. Finally, ABC should conduct annual gap analyses against NIST CSF to assess its Profile improvement year over year.

Remainder of page left blank intentionally.

Observations and Recommendations

The following recommendations, based on our technical cybersecurity assessment, are intended to improve the security and control of ABC's IT environment.

5

No. 1: Patch Management

NIST CSF Controls: PR.DS, PR.IP, RS.MI

We evaluated the patch management process by scanning the internal network using Nessus Professional. Based on the results of the scans (see finding No. 2, Internal Network Vulnerability Assessment and Penetration Test), it appears that the patch management process should be improved.

Potential Risk:

Without a documented and monitored patch management procedure, IT personnel may not apply patches consistent with management's intentions. Systems may remain unpatched for extended time periods, creating unnecessary security risks, such as system and data breaches.

Recommendation:

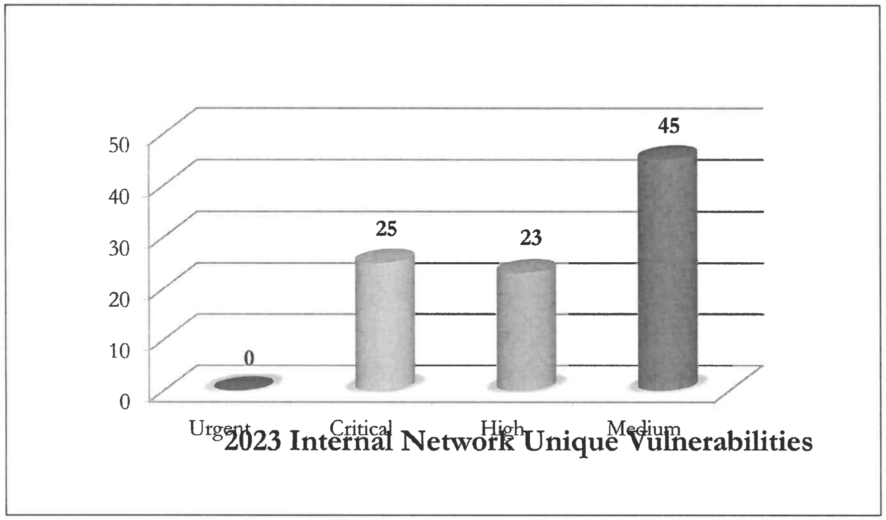
We recommend that ABC develop and implement a formal patch management process and supporting procedures. An effective patch management strategy includes the following items:

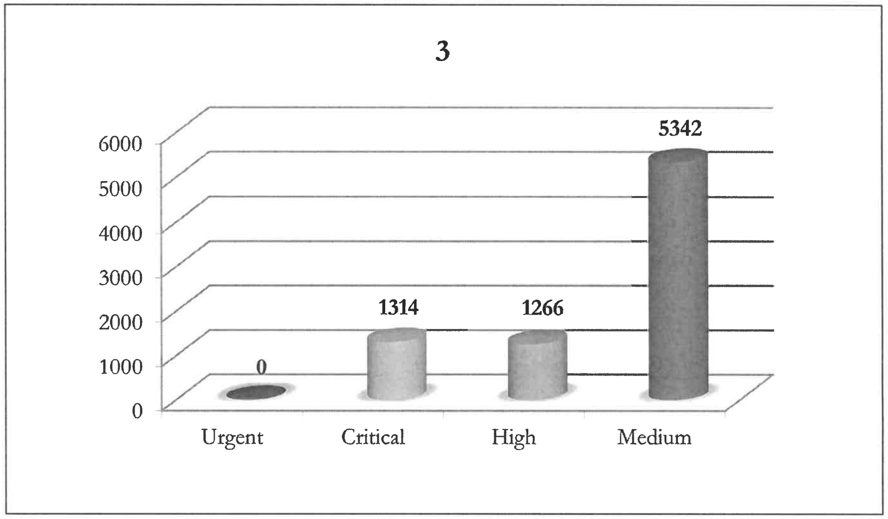
- Periodic standing change requests for patch-related changes. The standing change requests should point to a patch/patch exception log.
- A patch/patch exception log recording all patches. If a technology is used to manage patches, it should be configured to record all servers, workstations, databases, and devices patched and the specific patches applied. Legacy systems and systems that are part of a replacement plan are candidates for inclusion in the patch exception log. Also, in certain cases, patching a system that is supported by the vendor voids the support agreement. Systems like this should be included in the patch exception log.
- A robust patch management solution that is not technology-specific and supports virtual patch testing and exception patch management.
- Periodic reviews to ensure the process is followed.

No. 2: Internal Network Vulnerability Assessment and Penetration Test

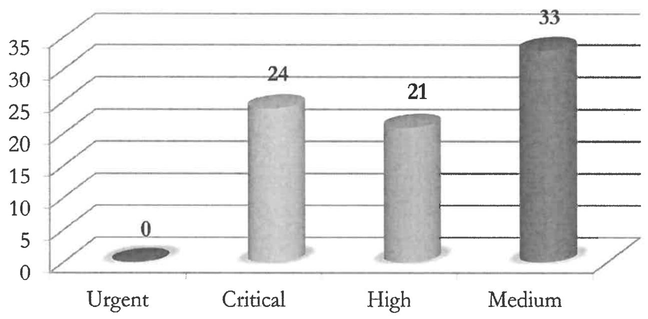
We scanned ABC's internal network and identified 25 critical-, 23 high-, and 45 medium-priority unique vulnerabilities. The scan results revealed vulnerabilities that increase the likelihood of an internal network breach.

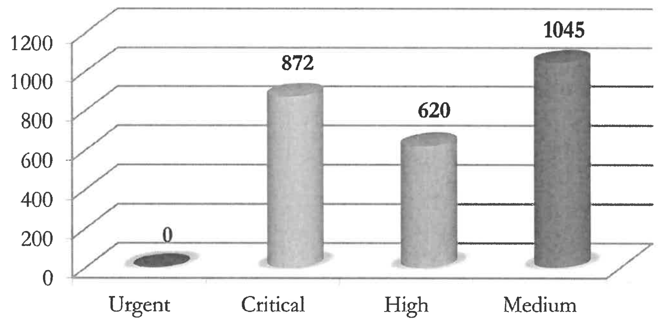
The charts below show the vulnerabilities we identified, prioritized by level of severity, as defined by the Common Vulnerability Scoring System, Version 3.0 (CVSS v3.0). The technician's report summarizes the unique vulnerabilities, affected systems, and recommended solutions. In many cases, the recommended solution requires a system security patch.





No. 2: Internal Network Vulnerability Assessment and Penetration Test (continued)


2023 Internal Network Unique Vulnerabilities*


2023 Internal Network Total Vulnerabilities*

*Excluding SSL and TLS vulnerabilities.

Securance analyzed the results of the internal vulnerability assessment to determine an effective penetration testing plan. We identified several hosts and systems to target during the penetration test. We presented the results to ABC's IT management, which assessed the list and approved penetration testing of the following systems.

No. 2: Internal Network Vulnerability Assessment and Penetration Test (continued)

Hostname | IP		Vulnerability Summary	Exploit Results
• XX.XX.XX.XXX • XX.XX.XX.XXX	• XX.XX.XX.XXX	NFS Mount Scanner	Exploit completed successfully.
• XX.XX.XXX.XX • XX.XX.XXX.XX • XX.XX.XXX.XX	• XX.XX.XXX.XX • 4 other vulnerable host not tested.	AXIS_SRV_Parhand_rce	Exploit completed successfully and command shell opened.
• XX.XX.XX.XX		Exchange Proxyshell	Exploit failed. However, all email addressed downloaded.
• XX.XX.XX.XX		MS12_020_Check	Host confirmed vulnerable.
• XX.XX.XXX.XX • XX.XX.XXX.XX • XX.XX.XX.XX	• XX.XX.XXX.XX • XX.XX.XXX.XX • XX.XX.XX.XX	PHP_CGI_ARG_Injection	Exploit completed successfully, but no session created. False positive.
• XX.XX.XX.XX • XX.XX.XX.XX		Tomcat JSP upload bypass	Exploit completed successfully, but no payload delivered.
• Multiple host		SMB Signing not required	No usernames or password hashes retrieved.

While our exploits targeting the hosts listed above were only partially successful, it is worth noting the following:

- We identified 1314 hosts with 25 unique critical vulnerabilities and 1266 hosts with 23 unique high vulnerabilities.
- A bad actor would not request approval to attempt exploits, would have unlimited time to deploy advanced persistent threat techniques, and might experience success. The details of our penetration testing efforts are in the technician's report.

No. 2: Internal Network Vulnerability Assessment and Penetration Test (continued)

Potential Risk:
As a result of our testing, we believe that ABC's internal network is at a critical risk of being compromised by an attacker. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, and data could be compromised.

Recommendation:
We recommend that ABC's IT staff address the critical-, high-, and medium-risk vulnerabilities and perform periodic internal network vulnerability scans.

Remainder of page left blank intentionally.

No. 3: Data and Information Security

The objective of a data and information security program is to prevent unauthorized access to, and use, disruption, modification, and destruction of, data assets. To achieve this objective, enterprises implement multiple layers of defense, including governance, technologies, and IT processes that contain controls based on best-practice frameworks. The following table lists security technologies and controls that Securance recommends to protect ABC's data assets.

Governance | Technology | IT Process Control	Current State
1. Governance: Cybersecurity Program	ABC currently aligns with NIST CSF. However, the program is informal and immature.
2. Governance: End-user Security Awareness Training	No effective training program in place. Attempts to implement formal end-user security awareness training have not been well-received within the organization.
3. Governance: IT Security Policy	Refer to finding No. 5: Policies and Procedures.
4. Governance: Data Classification Standard – Structured and Unstructured	There is a draft cybersecurity policy that contains data classification language. • Data assets within the organization have been identified, and their classifications have been documented. • Data ownership process is not in place. • Data classification is not supported across the organization. • There is no technology in place to enforce data classification.

No. 3: Data and Information Security (continued)

Governance | Technology | IT Process Control	Current State
5. Governance: Patch Management Policy/Procedure	• There is no patch management policy. • Patching frequency is inconsistent, with the exception of critical patches. • Select network equipment (e.g., firewalls) is maintained.
6. Technology: Next-Generation Firewall	Implemented CheckPoint 8R81.10.
7. Technology: Intrusion Prevention System (IPS)	Configured within a licensed module of the CheckPoint firewall.
8. Technology: Password Management	Standard password policy: • Minimum length – 8 characters • Complexity – enabled • History – 5 • Minimum Age – 7 days • Lockout – 3 attempts Privileged password policy: • Minimum length – 12 characters • Complexity – enabled • History – 10 • Minimum Age – 7 days • Lockout – 3 attempts
9. Technology: Data Encryption	The primary enterprise file server does not encrypt data at rest. However, there is confirmed sensitive data on the file server.
10. Technology: Data Loss Prevention (DLP)	No appliance-based DLP solution. However, DLP is implemented in a limited form via Mimecast email gateway.
11. Technology: User Behavior Analytics	Provide by Varonis and Extrahop technologies.

No. 3: Data and Information Security (continued)

Governance | Technology | IT Process Control	Current State
12. Technology: Multi-Factor Authentication (MFA)	• MFA implemented for University. Currently in a pilot program for technology staff. Plan in place to roll out to all employees and staff August 202X.
13. IT Process: User Provisioning – Unique User IDs	All user IDs are unique.
14. IT Process: User Provisioning – Periodic User Reviews	ABC does not perform periodic user reviews to confirm that active accounts are for current employees, and that account permissions match job duties.

Potential Risk:

The absence of a comprehensive data and information security strategy could result in unauthorized access to data, data exfiltration, or a network or system breach. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

Recommendation:

In addition to the recommendations associated with the other findings in this report, we also recommend that ABC:

- Formalize the cybersecurity program that is aligned with the NIST CSF. That can be accomplished by formalizing the cybersecurity policy and building out additional components of the program.
- Implement an end-user security awareness training program using content from an industry leader, such as KnowBe4. The training should be annual for all employees and supported by semiannual testing. Employees that fail the test should be required to take a refresher training.
- Implement a formal data classification program. In addition to the policy, ABC needs technologies to support the identification of data assets based on the classification standards. Additionally, the current Office 365 (O365) subscription provides tools to implement data classification across Microsoft Office products. ABC should investigate and implement these tools as a starting point for data classification.

No. 3: Data and Information Security (continued)

- Implement an effective patch management policy and procedures.
- Procure and implement a network file share that encrypts sensitive data at rest.
- Implement the DLP options provided with the current O365 subscription.
- Continue with the current plans to implement O365 MFA for technology staff, followed by a complete rollout to all employees. This would provide an additional layer of security for email authentication. Further, ABC's IT management should consider an MFA solution for access to internal network resources that contain sensitive information or are considered critical enterprise applications.
- Perform periodic reviews of all domain users. This will ensure that employees that are separated from ABC can no longer access technology resources and data assets.

Remainder of page left blank intentionally.

No. 4: Web Application Vulnerability Assessment
NIST CSF Controls: ID.AM, ID.RA, PR.AC, PR.IP, PR.PT, DE.AE, DE.CM, RS.AN, RS.MI

We performed a detailed security assessment of the following Internet-facing web applications. Our overall findings are summarized below, with specific vulnerabilities detailed in Appendix A:

- ABC Employee Contracts – https://www.xxxxx-x1.net – low risk of compromise based on the identified vulnerabilities.
- Safety Video Viewing/Tracking – https://www.xxxxx-x2.net– low risk of compromise based on the identified vulnerabilities.
- SIS Training Registration - https://www.xxxxx-x3.net - low risk of compromise based on the identified vulnerabilities.
- Admin Office Front Desk Sign-In – https://www.xxxxx-x4.net – low risk of compromise based on the identified vulnerabilities.
- Incident Reporting - https://www.xxxxx-x5.net – low risk of compromise based on the identified vulnerabilities.
- Retirement Counseling Registration – https://www.xxxxx-x6.net – high risk of compromise based on the identified vulnerabilities.
- Contact Forms – https://www.xxxxx-x7.net – moderate risk of compromise based on the identified vulnerabilities.
- Hotspot Request Form – https://www.xxxxx-x8.net – low risk of compromise based on the identified vulnerabilities.
- Web Request Form – https://www.xxxxx-x9.net – low risk of compromise based on the identified vulnerabilities.
- Student Information System – https://www.xxxxx-x10.net – moderate to high risk of compromise based on the identified vulnerabilities.

No. 4: Web Application Vulnerability Assessment (continued)

Potential Risk:

A successful attack could leave one or more web applications unresponsive or compromised data.

Recommendation:

Notwithstanding the layered security defenses protecting ABC's the web applications, we recommend that IT management address the high- and medium-risk vulnerabilities identified in Appendix A.

Remainder of page left blank intentionally.

No. 5: Policies and Procedures

We reviewed the following IT policies/governance documents:

Document Name	Type	Comment
1. Access Control Procedure	Procedure	Titled “procedure” but written as a policy. Content appears appropriate and adequate. No revision history. Mapped to control frameworks.
2. Cybersecurity Training and Awareness Policy	Policy	Refer to Access Control Procedure.
3. Data Sharing Agreement_2021_ABC	Agreement	Excellent governance document.
4. Draft - Cybersecurity Policy	Policy	We do not recognize the importance or value of this document. It references many other existing policies. In our opinion, a cyber resilience program (CRP) document would provide increased value to the organization.
5. Enterprise Password Procedure	Procedure	Contains all the components of an effective governance document.
6. Acceptable Use Policy	Policy	Excellent governance document.
7. Network Security Policy	Policy	Content appears appropriate. However, the policy lacks essential network security items, such as vulnerability management, intrusion detection/protection, deep-packet inspection, and DLP. No revision history. Mapped to control frameworks.
8. Risk Management Procedure	Procedure	Excellent governance document.

Except for the network security policy, the documents reviewed contain adequate language and are mapped to appropriate frameworks.

No. 5: Policies and Procedures (continued)

Potential Risk:

Without formal policies specific to ABC's IT environment to govern daily operations, staff may adopt operations consistent with their prior experience. While their intentions may be good, their actions may not be in line with IT management's desires.

Recommendation:

We recommend that ABC modify all policies and procedures to include revision history and disciplinary actions. Further, we recommend that the network security policy include language requiring vulnerability management, intrusion detection/protection, deep-packet inspection, DLP, and other measures to protect ABC's technology assets.

Additionally, we recommend that ABC develop a playbook to support the IRP, implement a CRP, and perform annual tabletop exercises.

Remainder of page left blank intentionally.

No. 6: Firewall Configuration Analysis

We performed a detailed configuration analysis of the following firewalls and noted the following:

- CheckPoint 23800 Security Gateway (OS: R81.10):
    - Licensing includes VPN, mobile access, application control, URL filtering, identity and content awareness, and threat prevention. Secure socket layer (SSL) deep inspection is noticeably absent.
    - The IPS policy is appropriately configured.
    - Noted fewer than six rules that should be deleted, as they are no longer used. However, these rules do not present unnecessary risks to ABC.
- Fortigate-1 – did not identify rules or configurable items that pose unnecessary risks to ABC.
- Fortigate2 – did not identify rules or configurable items that pose unnecessary risks to ABC.
- Fortigate3 – did not identify rules or configurable items that pose unnecessary risks to ABC.
- Fortigate3 – did not identify rules or configurable items that pose unnecessary risks to ABC.Fortigate – vpn-abc.fortigate – did not identify rules or configurable items that pose unnecessary risks to ABC.

<u>Potential Risk:</u>

Our assessment indicates that ABC's network is at a low risk of being compromised due to a security risk or exploitable weakness in its firewalls. If the network were attacked, depending on the type of attack and its level of success, systems could be rendered unresponsive, and data could be compromised.

<u>Recommendation:</u>

We commend ABC's IT management for streamlined firewall configurations. We still recommend periodic third-party reviews to ensure that the firewall configurations remain as secure as practical.

No. 7: Wireless Network Assessment (Juniper Mist)

NIST CSF Controls: ID.AM, ID.RA, PR.AC, PR.IP, PR.PT, DE.AE, DE.CM, RS.AN, RS.MI

During our site visit, we identified a cloud-managed controller that authorizes access to the following service set identifiers (SSIDs):

SSID	Level of Access	Internet	Internal Network	Encryption/ Security	User Authentication	Device Authentication
ABCWN	Internet and Internal Network	✓	✓	AES	WPA2-Enterprise (Radius)	No
guest-ABC	Internet Only	✓		None	Open	No
STAFFBYOD	Internet Only	✓		None	Captive Portal to Microsoft Login	No
VendorNet	Internet Only Staff Support Center	✓		AES	WPA2	No
CLASSVR-ABC	Internet Only	✓		AES	WPA2	No

As part of our review, we also noted the following:

- The wireless network's native logs are retained in the cloud for a rolling 30-day period but are not ported to a central log server.
- Rogue access point detection is enabled.
- Wireless access to the business network is segmented via a separate VLAN.

Potential Risk:

The wireless network is at a low risk of being used by an attacker or unauthorized user to compromise ABC's technologies. If a breach were to occur, the network could be rendered unresponsive, or an unauthorized user could access information resources.

No. 7: Wireless Network Assessment (Juniper Mist) (continued)

Recommendation:

We recommend that ABC’s IT management implement device authentication and a process to identify and remove rogue access points.

Remainder of page left blank intentionally.

No. 8: External Network Vulnerability Assessment

NIST CSF Controls: ID.AM, ID.RA, PR.AC, PR.IP, PR.PT, DE.AE, DE.CM, RS.AN, RS.MI

We scanned ABC's external network and identified eight medium-priority unique vulnerabilities. The scan results did not reveal vulnerabilities that increase the likelihood of an external network breach.

The charts on the following page show the vulnerabilities we identified, prioritized by level of severity, as defined by CVSS v3.0. Appendix A summarizes the unique vulnerabilities, affected systems, and recommended solutions. In several cases, the recommended solution requires a system security patch.

Potential Risk:

As a result of our testing, we believe that ABC's external network is at a low risk of being compromised by an attacker. If a breach were to occur, depending on the type of breach, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems.

Recommendation:

We recommend that ABC's IT staff address the medium-risk vulnerabilities and perform quarterly external network vulnerability scans.

Vulnerability details are provided in a separate technician's report. Low-risk vulnerabilities and informational disclosures are only provided in the technician's report. A finding and technical vulnerability legend is provided on page 5.

No. 9: System IoCs

We assessed a sample of servers for IoCs. Our selection was strategic and based on common system attack vectors. Most attackers target endpoints and/or end users to breach enterprise networks. Once inside, they attempt to move laterally and obtain access to directory service, file, and/or database servers, which are typically high-value targets. For this reason, we ran a suite of vulnerability scanners and forensic tools against the following servers:

1. Domain controller (hostname: SSC-DC01 | XX.XX.XX.XX)
2. Database server (hostname: SSC-FS1 | XX.XX.XX.X\X)
3. File server (hostname: SQL | XX.XX.X.XX)

We gathered data from each system related to program execution, registry, file folder opening, file downloads, deleted files, file knowledge, location, external devices, account usage, browser usage, and persistence. We analyzed this data for information that appeared abnormal, on multiple systems, or otherwise out of place.

We did not identify IoCs on any of the three systems listed above. While our assessment did not cover the entire technology environment, we can reasonably conclude that ABC's layered security defenses are effective.

<u>Potential Risk:</u>

Though we did not identify IoCs, attack surfaces, hacking techniques, risks, and threats are constantly evolving. ABC must remain vigilant to continue protecting its technologies from compromise. Depending on the breadth and depth of compromise, bad actors can leverage a single attack to obtain password hash files, exfiltrate data, and/or establish reentry points.

<u>Recommendation:</u>

We commend ABC for implementing layered security defenses. We recommend that ABC remain vigilant, address the technical findings in this report, and continue to perform periodic security assessments.

No. 10: Firewall Optimization

NIST CSF Controls: None

We identified several opportunities to streamline the FortiGate firewall configurations:

Firewall	XXX	XXXX	XXXXXX	XXXXX	XXX-XXXX
• Rules	3	37	32	36	44
• Services	249	259	251	253	247
• Host Groups	108	154	87	146	135
• Covered Rules	1	0	3	30	0
• Redundant Rules	0	1	1	0	7
• Consolidate Rules	0	1	1	0	3
• Rules No Remarks	2	33	32	34	23
• Unattached Objects	32	49	14	23	57
• Duplicate Objects	1	2	1	1	12

Potential Risk:

The above items represent housekeeping tasks that should be performed to ensure that the firewalls function optimally. Leaving these items unresolved provides opportunities for network breaches, confusion, and/or potentially excessive access.

No. 11: Website and Web Application Housekeeping

NIST CSF Controls: None

We identified a named email address in one of the web applications (https://trusted.abc.k12.us:1234/register/register.jsp). Named email addresses facilitate social engineering via email phishing.

Potential Risk:
Removing named email addresses is a housekeeping task that helps maintain secure, streamlined web applications and prevent email phishing.

Recommendation:
We recommend that ABC remove all email addresses that name specific users.

Remainder of page left blank intentionally.

No. 12: External Network Public Information

We searched for publicly available information about ABC's Internet-facing (external) network and found that the American Registry for Internet Numbers (ARIN) identifies XX.XXX.XXX.X/XX as being registered to Cox Communications. The registry information provided by ARIN is appropriately cleansed of ABC-specific information, such as names and email addresses.

We also searched the "surface web," social media sites (Glassdoor, Facebook, Instagram, YouTube, Twitter, and LinkedIn), and the "dark web" (i.e., .onion), using the TOR browser and multiple sites (ahmia.fi, The Hidden Wiki, TORCH, and Candle), and found information about ABC's technology environment.

Potential Risk:

Public information about an organization's Internet-facing network is both unnecessary and an entry point for attackers.

Recommendation:

We recommend that ABC confirm that the password syntax has been updated. This is a method of confirming that the email address and password combinations are dated. In addition, we recommend that ABC periodically review IP address registrations, the surface web, and the dark web to ensure all available information is properly sanitized.

Remainder of page left blank intentionally.

SECURANCE VALUE

Securance Consulting would like to THANK YOU for your business. Aside from benefiting from the highest level of service possible, you also received unique advantages that only Securance Consulting delivers. Our hands-on approach is tailored to fit the needs of the information technology department. Our technical expertise, outstanding reputation and personalized attention ensure you receive a level of service that no other cybersecurity firm can surpass.

As a Securance customer, you can be confident in your decision to manage technology risk by partnering with Securance!

APPENDIX A: TECHNICAL VULNERABILITY SUMMARIES

NO. 4: WEB APPLICATION VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Threat Level	Web App	Vulnerability Family	Fix | Recommendation
High	• Retirement Counseling • Student Information System	Possible Blind SQL Injection Fault Found	Possible False Positive: Sanitize all user input.
Medium	• Employee Contracts • Admin Office Sign-In • Retirement Counseling • Contact Forms • Student Information System	Application Appears Susceptible to Clickjacking Attacks	Add the following HTTP header to your server's response: X-FRAME-OPTIONS: DENY or X-FRAME-OPTIONS: SAMEORIGIN (if you want to allow it only under the same domain context).
Medium	• Employee Contracts • Student Information System	Found an Insecure Cookie for Scripting (no HttpOnly Enabled)	Enable HttpOnly according to your web platform instructions.
Medium	• Student Information System	Webserver Does Not Provide Support for SSL/TLS Forward Secrecy Cipher (PFS)	Enable Perfect Forward Secrecy.
Medium	• Safety Video Viewing • SIS Training Registration • Incident Reporting • Web Request Form	Found an Invalid SSL Certificate (Mismatched Common Name)	Possible False Positive: Obtain a valid certificate.

Threat Level	Web App	Vulnerability Family	Fix | Recommendation
Medium	• XXX	Found an Invalid SSL Certificate	Obtain a valid certificate.
Medium	• XXX	Possible Backup File Found	Remove all backup files from the webserver.
Medium	• Employee Contracts • Admin Office Sign-In • Retirement Counseling • Student Information System	Multiple Cross-Site Request Forgery Vulnerability Found	Most prevention techniques work by embedding additional authentication data into requests that allows the web application to detect requests from unauthorized locations.
Medium	• XXX	Possible HTTP Parameter Pollution Vulnerability Has Been Found	Sanitize user's input.
Medium	• Employee Contracts	Web Form Allows Password Caching (Autocomplete = on)	Disable autocomplete.
Medium	• Admin Office Sign-In	Possible Cross-site Scripting and/or HTML Injection Found	Parse user's input before inserting it directly to be rendered into client-side browser.
Medium	• Contact Forms	Possible SQL Error Handling Fault has been found	Sanitize user's input.

SECURANCE CONSULTING

Advantage of Insight | AI

13916 Monroes Business Park, Suite 102 • Tampa, FL 33635
www.securanceconsulting.com