BOARD MEETING DATE: 3/18/2025

ITEM NO: XII-a

RECOMMEND THAT the Board approves the agreement with Security Compliance Associates in the amount of $7,200.00 for IT penetration testing.

SCA
SECURITY COMPLIANCE ASSOCIATES

MASTER SERVICES AGREEMENT
Standard Terms and Conditions

Security Compliance Associates, a Financial Institution Information Security Compliance, Company FIISC L.L.C., whose principal office is located in Clearwater, Florida (hereinafter "SCA"), and North Florida College, (hereinafter "Client") whose principal office is located in Florida, hereby enter into, as of the date set forth below (the "Effective Date"), this Master Services Agreement (the "Agreement") consisting of the Standard Terms and Conditions and the following Exhibits and Service Deliverable Attachments marked below, which are attached hereto and incorporated herein for all purposes.

Master Services Agreement Standard Terms and Conditions

Exhibits

Exhibit A	Services and Fees …………………………………………………………………………..	**X**
Exhibit B	Cybersecurity Assessment and Advisory Services Proposal Dated 01.13.2025 ……..	**X**

1. INTRODUCTION

SCA is an active Florida Company engaged in the business of providing Information Security Assessment and Compliance Advisory Services to organizations who store, process, or maintain sensitive information.

2. TERM AND TERMINATION

This Agreement shall commence as of the Effective Date and shall remain in effect for one year thereafter unless either party not then in breach of this Agreement, at its sole option, for any reason or for no reason, terminates the agreement by giving written notice to the other party at least thirty (30) days prior to termination. Client will have the option of continuing the selected services in subsequent years under the same terms and conditions with written notification.

3. SCOPE OF SERVICES

In consideration of the fees described in Exhibit A of this Agreement, SCA will provide those services selected by Client and further described in the Attached Proposal as part of this Agreement, which are attached hereto and incorporated herein for all purposes. Additional services may be added during the Agreement term through approval of both parties of a Statement of Work for such service as an Addendum to this Agreement.

4. FEES AND PAYMENT TERMS

Upon acceptance of Master Services Agreement by Client, SCA shall invoice Client according to the payment schedule described in Exhibit A, which is attached hereto and incorporated herein. The client agrees to pay SCA the amount invoiced, including applicable taxes, upon receipt of invoice. The client also agrees to pay all expenses related to the printing of all requested documents. The fees specified in Exhibit A are the total fees and charges and will not be increased during the term of this Agreement except as the parties may agree in writing.

5. OBLIGATIONS OF SECURITY COMPLIANCE ASSOCIATES

a) Qualified employees of SCA shall perform those services selected by Client and further described in the Service Deliverable Attachment(s) marked on Page 1 of this Agreement.

b) A qualified employee shall be available and will reply to Client, within four hours Monday through Friday, between the hours of 9:00 a.m. and 5:00 p.m. Eastern Time, excluding legal holidays, to schedule any request for services under this Agreement. Cell phone numbers may be exchanged to offset time zone difference.

c) SCA will ensure that its employees and agents will, whenever on Client's premises, obey all reasonable instructions and directions issued by Client.

6. OBLIGATIONS OF CLIENT

a) When SCA provides services at Client's facility, Client shall provide SCA reasonable working space and access to facilities and systems as required for timely performance of services.

b) Client agrees to make available to SCA upon reasonable notice, computer programs, data, and all other documentation required by SCA to complete the services and will be entitled to rely upon the accuracy and completeness of that data and materials and the conformity of materials indicated as representative of the normal and customary course of business.

c) Client agrees to adhere to scheduled project dates. Scheduled projects delayed within 30 days of committed resources, due to factors within reasonable control of Client, are subject to fees to partially recover lost costs, not to exceed $100 per hour. Each occurrence will be communicated and negotiated as required.

7. WARRANTIES

SCA warrants that Services provided will be performed in a professional and workmanlike manner consistent with the level of care and skill ordinarily exercised by members of SCA's profession currently performing such services under similar conditions. SCA will remedy any noncompliance with the foregoing at no cost to Client.

SCA warrants that each Service Deliverable will contain all of the features and/or perform as stated in this Agreement and the Service Deliverable Attachment(s) marked on Page 1 of this Agreement. SCA will remedy any noncompliance with the foregoing at no cost to Client.

SCA warrants that Services and Deliverables will not infringe on the copyright, patent or trade secret of any third party. If any portion of the Services or Deliverables supplied hereunder fails to comply with this warranty against infringement, SCA hereby agrees to indemnify, protect, defend, and hold Client harmless from all claims, suits, actions, and judgments which may be sustained by Client as a result of such failure; provided, however, that (i) Client gives written notice of any such claim or suit to SCA within thirty (30) days of receiving notice of such claim or suit, and (ii) SCA shall have sole control of the defense of any action or claim and all negotiations for settlement or compromise thereof. The client may elect to participate in any such action with an attorney of its own choice and at its own expense. In the event Client is precluded by a court of competent jurisdiction from using any Deliverable as a result of such an infringement, SCA may, in its sole and absolute discretion, (i) obtain the right to use the Deliverable for Client, (ii) replace or modify the Deliverable so that they no longer infringe or terminate this Agreement with a pro-rata refund of the fees received by SCA from Client. If Client fails to notify SCA as required herein, or if Client or its agents have modified any Deliverable from the form delivered by SCA, or combined it with any other work, Client's rights under this section shall terminate.

8. CONFIDENTIALITY

Each party acknowledges that it may receive confidential information and / or trade secrets ("Confidential Information") from the other party while performing the Services and developing the Deliverable. Each party shall maintain the confidentiality of the other party's Confidential Information and shall not sell, license, publish, display, distribute, disclose, or otherwise make available such Confidential Information to any third party nor use such Confidential Information except as authorized by this Agreement. Notwithstanding the foregoing, information that either party can document is in the public domain and generally available for use and disclosure by the general public without change or license shall not be considered Confidential Information within the meaning of this Agreement, and therefore the above restrictions on use and disclosure of confidential Information will not apply to any such information and neither party shall be liable for disclosure or use of any such information.

It is understood and agreed that SCA may use software, documentation or information that is proprietary to SCA ("Proprietary Information") in providing services. If SCA uses any such Proprietary Information, Client shall not market or in any way use Proprietary Information in contravention of this Agreement. Client shall not acquire any ownership rights to such Proprietary Information and Client shall not sell, transfer, publish, disclose, display, or otherwise make available the Proprietary Information. Client agrees to secure and protect the Proprietary Information in a manner consistent with the maintenance of SCA's rights and to take appropriate action by instruction or agreement with its employees and / or consultants who are permitted access to such information to satisfy its obligations hereunder.

SCA acknowledges that it may receive confidential and nonpublic personal information about Client during this agreement. SCA warrants that SCA, its officers, employees and agents will (a) hold in strictest confidence all information related to Client (b) not to use such information for any purpose other than providing the services set forth in this Agreement, and (c) not provide any information about Client, Client's members to any third party without Client's prior written consent, except as permitted by applicable federal and state laws and regulation, as amended from time to time. All information provided by the Client to SCA during the term of this Agreement shall remain the property of Client and shall be returned to Client or destroyed in accordance with SCA Information Security Policy upon termination of the Agreement. All warranties set forth in this paragraph shall survive termination of this Agreement

9. COMPLIANCE

Throughout the term of this Agreement by and between SCA and Client, SCA will remain in compliance with Federal laws and regulations governing the privacy and security of sensitive, non-public information, including but not limited to the Gramm-Leach-Bliley Act (Public Law 106-102 – November 12, 1999) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). SCA has established, implemented, and maintains, a comprehensive information security program which includes administrative, technical, and physical safeguards designed to : (1) Ensure the security and confidentiality of consumer records and information; (2) Protect against any anticipated threats or hazards to the security or integrity of such records and information; (3) Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any consumer; (4) ensure the proper disposal of consumer information; and (5) provide appropriate response to unauthorized access to or use of sensitive consumer information.

Furthermore, SCA will comply with all state laws in the jurisdiction in which Client maintains its principal place of business and federal laws and regulations addressing the privacy and protection of nonpublic personal information as those laws or regulations may be enacted or amended throughout the term of this Agreement. SCA will adjust its information security program as necessary, due to changes in technology, changes in the sensitivity of the information SCA maintains or has access to, or changes in law or regulation, during the term of this Agreement with Client. SCA will allow periodic, reasonable audits of its business processes to validate performance under the contract provisions.

10. LIABILITY AND INDEMNIFICATION

SCA shall indemnify, defend, and hold harmless Client and its officers, employees, members, and agents, in their individual capacities or otherwise, from and against all losses resulting from, arising out of, or incurred in connection with: SCA's gross negligence or willful misconduct, SCA's misuse of software or services, SCA's failure to comply with applicable law or regulation, or infringement of any trademarks, copyrights, patents, or other intellectual property caused by SCA.

Client shall indemnify, defend, and hold harmless SCA and its officers, employees, members, and agents, in their individual capacities or otherwise, from an d against any and all losses resulting from, arising out of, or incurred in connection with: Client's gross negligence or willful misconduct, Client's misuse of software or services, Client's failure to comply with applicable law or regulation, or infringement of any trademarks, copyrights, patents, or other intellectual property caused by Client.

11. LIMITATION OF LIABILITY

Except as provided in this Agreement, SCA shall not be liable to Client or any other person, firm, or corporation for any loss or special, indirect, incidental, consequential, or punitive damages, including, without limitation: lost profits, loss of time, money, data, or goodwill, or any other claim or demand by or against Client which may arise out of the furnishing, performance or use of any item or service provided under this Agreement and Client shall hold SCA harmless from any such claim. In no event shall SCA's total liability exceed $1,000,000.00.

12. MISCELLANEOUS

A. This Agreement, including the Exhibits and Service Deliverable Attachments <u>marked</u> on Page 1, which are attached hereto and incorporated herein constitutes the entire agreement between the parties in relation to the services, and (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communication between the parties during the term of this Agreement.

B. If any provision of this Agreement is held invalid, all other provisions shall remain valid unless such validity would frustrate the purpose of this Agreement, and this Agreement shall be enforced to the full extent allowable under applicable law.

C. No modification to this Agreement is binding, unless in writing and signed by a duly authorized representative of each party.

D. From time to time, scrivener's errors may arise in creation of an Agreement and/or the Agreement's respective Exhibits, Proposal(s) and SOW(s). Scrivener's errors can include typing an incorrect word, number or letter, or omitting a word or words. SCA will not be held liable for scrivener's errors that do not materially affect the Agreement and will communicate any such errors found with the Client. Client may request revised documents to correct found errors. Corrected documents are subject to item C above.

E. SCA shall not be liable for any delay in performance due to force majeure, including strikes, accidents, acts of God, acts of terrorism or other delays beyond the control of SCA. If timely completion of the Services is prevented by any cause of force majeure, or any act of Client, then such failure or delay shall not constitute default or breach of contract.

F. The Agreement shall be subject to and governed by the laws of the State of Florida, although one or more of the parties now is or may become a resident of a different state. The client agrees to submit itself to the jurisdiction of the courts of the State of Florida for any action arising out of this contract. The jurisdiction and venue for any such action shall be Pinellas County, Florida.

G. The marginal headings of the paragraphs of the Agreement and attached Exhibits are for convenience only and are not to be considered a part of the Agreement or used in determining its content or context.

H. Any modification or amendment of the Agreement shall be in writing and shall be executed by all parties.

I. The provisions of the Agreement shall inure to the benefit of and be binding upon the parties thereto, their heirs, executors, administrators and permitted assignees.

J. Any waiver by any party of a breach of any provision of the Agreement shall not operate as or be construed as a waiver of any subsequent breach thereof.

K. Execution of Agreement. This Agreement may be executed in any number of counterparts, each such counterpart being deemed to be an original instrument, and all such counterparts shall together constitute the same agreement. The exchange of copies of this Agreement and of signature pages by facsimile transmission shall constitute effective execution and delivery of this Agreement as to the parties and may be used in lieu of the original Agreement for all purposes. Signatures of the parties transmitted by facsimile shall be deemed to be their original signatures for all purposes.

L. Prevailing Party. If any party brings any judicial action or proceeding to enforce its rights under this Agreement, the prevailing party shall be entitled, in addition to any other remedy, to recover from the losing party, regardless of whether such action or proceeding is prosecuted to judgment, all costs and expenses, including without limitation reasonable attorneys' fees, incurred therein by the prevailing party.

M. Entire Agreement. This Agreement and the schedules and exhibit hereto, constitute the entire agreement among the parties with respect to the subject matter hereof and supersede all prior agreements and understandings, both written and oral, among the parties with respect to the subject matter hereof.

IN WITNESS WHEREOF, the duly authorized representatives of Client and SCA have executed this Agreement as of ____________________, (the “Effective Date”)*.

**Invoicing and scheduling of services will commence on or after the effective date*

Security Compliance Associates

By: James Catrett
(Authorized Signature)

Name: James Catrett________________

Title: Chief Operations Officer_________

Date:______________________________

Address:

5225 Tech Data Drive, Suite 200

Clearwater, FL 33760

Telephone: 727-571-1141

North Florida College

By:______________________________
(Authorized Signature)

Name: Dani Mays

Title:______________________________

Date:______________________________

Address:

325 NW Turner Davis Dr., Ste A

Madison, FL 32340

Telephone: 850-973-2288

Accounts Payable/Invoicing Contact:

Name:______________________________

Email:______________________________

PO#:___P0023053_________________
(if applicable)

Project/Technical Contact:

Name:______________________________

Email:______________________________

Service and Fees (Exhibit A)

Description	Annual Qty.	Unit Cost	Total
External Network Penetration Testing White Box, 25 IPs, 16 Hours	1	$3,600	**$3,600**
Remediation Validation Re-Testing Network	1	$3,600	**$3,600**
Total Project Fees:			**$7,200**
Fees are valid for sixty (60) days from the date of this proposal			

Terms:
1. 50% of the Total Project Fees ($3,600) is due on the “Effective Date” of Master Services Agreement.
2. Balance ($3,600) due six months after “Effective Date” or at project completion, whichever occurs first.
3. Travel, if needed, is invoiced separately at actual cost.
4. All invoices are due upon receipt.
5. Remittance by ACH (preferred), Check or Credit Card (4% Fee for Credit Card).

North Florida College may elect a multiple year Agreement for annual service delivery. In consideration for a multiple-year Agreement, SCA will maintain the above fees for up to 3 years, unless changes to the project scope or economic conditions require a fee adjustment. Multi-year agreements are invoiced bi-annually in 50% installments.

SCA

SECURITY COMPLIANCE ASSOCIATES

CYBERSECURITY ASSESSMENT AND ADVISORY SERVICES PROPOSAL

FOR

NFC

NORTH FLORIDA COLLEGE

January 13th, 2025

Table of Contents

Executive Summary

North Florida College is a member of the Florida College System and accredited by the Southern Association of Colleges and Schools Commission on Colleges. NFC proudly serves the distinct educational needs of its six-county district, including Hamilton, Jefferson, Lafayette, Madison, Suwannee and Taylor counties, and beyond. NFC is well known for its comfortable campus setting, supportive environment and attention to student success.

Security Compliance Associates (SCA) is dedicated to delivering exceptional services that foster loyalty. Our clients can attest to our ability to conduct high-quality assessments while respecting their unique cultures. We appreciate your consideration of this proposal and want you to know that we are here to assist with any questions or clarifications you may have.

At SCA, we take pride in building strong partnerships with our clients, working closely with them to ensure mutual success. We see this engagement as the start of a long-term relationship as your security partner, rather than just a service provider. We respond to inquiries in a personal and straightforward manner, using clear and accessible language. With the extensive experience of our team, SCA stands out as one of the most knowledgeable providers in the industry.

SCA tailors its approach to meet client preferences for sharing results, emphasizing transparency. While each project is unique, we have experience engaging with management, IT, internal audit teams, committees, and even board members. Our reports are comprehensive and segmented by assessment phases, providing detailed summaries and priorities on security risks, vulnerabilities, recommended countermeasures, and corrective actions.

North Florida College seeks to evaluate the security of their external network by subjecting them to simulated real-world attacks.

To accomplish the above, SCA will provide extensive External Network Penetration Testing services to allow North Florida College to gain the best understanding of potential vulnerabilities, evaluate current controls to ensure information security and enhance the overall effectiveness of the cybersecurity and information protection program.

Company Overview

Security Compliance Associates, an Authorized HITRUST CSF® External Assessor, GSA contract holder, and Cyber AB Registered Practitioner Organization was formed in June of 2005.
SCA personnel have performed over 3,000 individual information security engagements nationwide. These engagements include security audits, CISO services, security consulting services, vulnerability assessments, penetration testing, application assessments, policy development, physical security, social engineering, information security training, controls review, NIST 800-53, 800-171, CMMC, CSF, ISO27001 (including ISO 27002 27005), PCI-DSS, Privacy Framework, GDPR, Risk Assessment and Management (800-30, 800-37, ISO 27005), HIPAA/HITECH, HITRUST CSF assessments and more.

SCA Project Staffing Team Leaders, who are introduced later in this proposal, and senior information security analysts are some of the best in the industry! Our analysts have been with us for 7 years on average and have additional experience before joining SCA.

Qualifications of our staff include:

- CISSP – Certified Information Systems Security Professional
- C|CISO - Certified Chief Information Security Officer
- CISA – Certified Information Systems Auditor
- CISM – Certified Information Security Manager
- CRISC – Certified in Risk and Information Systems Control
- CCSFP – Certified CSF Practitioner
- Cyber AB CMMC Registered Practitioner / Advanced Registered Practitioner
- ISO 27001 Lead Auditor
- C|EH – Certified Ethical Hacker
- Security+
- PenTest+
- PNPT – Practical Network Penetration Tester
- GMOB -GIAC Mobile Device Security Analyst
- GWAPT – GIAC Web Application Penetration Tester
- PMP – Certified Project Management Professional

Additionally, most of our senior analysts have earned a graduate degree in a related discipline including:

- Master of Science in Cybersecurity
- Master of Science in Digital Forensics
- Master of Science Information Technology
- Master of Science in Computer Information Systems

With more than 18 years of experience in delivering world class IT Information Security Assessment and Compliance services throughout the United States, our professionals bring over 200 years of combined Information Security experience, including the Department of Justice, Department of Defense and the National Intelligence Community.

SCA is proud of our 'hands-on – relationship first' approach to providing our comprehensive suite of industry-leading security compliance services. We work in partnership with our clients' executive, information technology, risk management and audit functions in the process of delivering superior services and results. This close interaction ensures a high level of satisfaction and knowledge transfer throughout the engagement. Helping our clients meet their objectives and safeguard critical information while complying with cybersecurity regulatory requirements are the sole focus of SCA.

Security Compliance Associates is a GSA contract holder, number 47QTCA20D008C, to deliver Highly Adaptive Cybersecurity Services (HACS). Cage Code: 74NW7. DUNS 014545808.

GSA Contract Holder
47QTCA20D008C

SCA is active in and supports the following information security organizations:

(ISC)²® ISSA Information Systems Security Association International ISACA® INFRAGARD PARTNERSHIP FOR PROTECTION

Since we are privately held with no shareholders or private equity investors to satisfy, we can deliver world-class services for reasonable fees. In other words, SCA delivers big name/big 4 skill sets without the big cost.

Thank you for accepting this information!

Respectfully,

The SCA Team

Scope, Approach and Methodology

In line with the principles of advanced IT certifications such as CISSP, CISA, CCSFP, and C|EH, Security Compliance Associates (SCA) is committed to staying informed about new and emerging threats to networks and environments, as well as current and evolving regulations. We leverage a combination of commercially available tools, proprietary software, and continuous education to fulfill our responsibilities. Given the diversity of our client base, we possess an extensive understanding of systems, platforms, and networks that is unmatched in the industry.

SCA typically collaborates directly with designated staff to tailor our services according to preferences outlined in this proposal. Please refer to the service descriptions for additional information. We encourage North Florida College personnel to actively participate in various aspects of the assessment process to promote knowledge sharing and understanding.

Our methodology adheres to a strict four-stage process for all engagements, based on NIST guidelines, which ensures a measurable, repeatable, and defensible approach as illustrated below:

PLANNING AND SCOPING

Define Objectives:

Establish the goals and objectives of the Assessment.

Scope Definition:

Clearly outline the systems, networks, and processes to be assessed.

Resource Allocation:

Identify and allocate the necessary resources, including personnel, tools, and documentation.

Schedule and Milestones:

Develop a timeline with key milestones and deliverables.

PENETRATION TEST METHODOLOGY

Reconnaissance

Research targets in scope through OSINT. Discover what is online and what is running on the hosts.

Testing/Exploitation:

Utilize tools and manual techniques to identify potential vulnerabilities and exploit.

Post Exploitation:

Dive deeper into compromised assets to demonstrate the true impact of a potential breach.

REPORTING AND RECOMMENDATIONS

Reports Compilation:

Compile findings into a comprehensive report, detailing vulnerabilities, risks, and impacts.

Prioritize Risks:

Rank risks based on severity and potential impact on the organization.

Recommendations:

Provide actionable recommendations for mitigating identified risks and vulnerabilities.

REPORTS DELIVERY AND FOLLOW-UP

Draft Reports:

Draft reports are provided to allow for client feedback and reports modification

Final Reports:

Once the organization and SCA have agreed upon the content, findings and recommendations, final reports are issued

Follow-up:

Upon request, SCA analyst presents the reports to the management and provides additional guidance as needed.

Penetration Testing Services

External Network Penetration Testing:

- SCA will conduct all requirements remotely via our Penetration Testing/Ethical Hacking Team.

North Florida College’s information technology and/or information security personnel are invited to “look over our shoulder” during the assessment as feasible, with data protection and privacy of utmost importance. Each engagement is an opportunity to facilitate transfer of knowledge within the time and scope of the project.

Details/targets of North Florida College’s environment for this engagement include (supplied by North Florida College):

Main Location: 325 NW Turner Davis Dr, Ste A Madison, Florida 32340, United States

Employees: 131

External IPs: 25

Servers: 17

IDS/IPS/Firewall: Fortinet

Network Penetration Testing

Penetration testing subjects systems to real-world attacks to gain system access or obtain sensitive information. SCA's standard penetration testing is performed as a White Box exercise where we have full knowledge of target systems and IP addresses in-scope. Grey Box (partial knowledge) and Black Box (zero knowledge) penetration testing are also available. Each requires increasing amounts of Planning and Discovery effort to identify target assets.

The phases of penetration testing include:

- Planning
- Discovery
- Attack - Exploitation
- Reporting
- Remediation Validation

The SCA Ethical Hacking Team is comprised of cybersecurity penetration testers from a variety of backgrounds who are all U.S. based, full-time employees of SCA. Certifications held by our Ethical Hacking Team include; CISSP (Certified Information Systems Security Professional), GWAPT (GIAC Web Application Penetration Tester), GMOB (GIAC Mobile Device Security Analyst, C|EH (Certified Ethical Hacker), Security+, PenTest+ and more. All Ethical Hacking Team members are required to continuously research and practice attack methodologies and pursue additional certifications. We do this to keep our skills current while learning the latest tips and tricks of the penetration testing trade.

Penetration testing frameworks and best practices used during engagements include the following:

	Description
Frameworks and Best Practices	• NIST SP 800-115 Technical Guide to Information Security Testing and Assessment • PTES - Penetration Testing Execution Standard • OSSTMM - Open Source Security Testing Methodology Manual • PTF -The Penetration Testing Framework • OWASP Web Security Testing Guide

	Description
Vulnerability Sources	• Common Vulnerabilities and Exploits (https://cve.mitre.org/data/refs/refmap/source-OSVDB.html) • Exploit Database (*https://www.exploit-db.com/*) • Microsoft Security Advisories (*www.microsoft.com/security*) • GitHub Repositories • OWASP Web Security Testing Guide (https://owasp.org/www-project-web-security-testing-guide/)

The reality is that an attacker could potentially spend days, weeks or months trying to compromise your systems while your business must operate with finite resources, including time and budget, to fend off malicious actors. Recognizing this, SCA penetration testing is delivered as best effort within a finite amount of time. To accomplish this, we will ask specific scoping questions appropriate for the type of testing (white, grey or black box) to determine an appropriate amount of time (hours) for the project.

SCA penetration testing is designed to not disrupt systems and is normally conducted during business hours. More hosts are active during business which allows our penetration testing to produce richer results to help you prevent exploitation in the future. Upon client request in advance during scoping, SCA will perform penetration testing after business hours or on weekends (a fee premium applies).

External Network Penetration Testing

External penetration testing is a practice that assesses the externally facing assets for an organization. During an external penetration test, the assessor attempts to enter the internal network by leveraging vulnerabilities discovered on the external assets. Below are the steps, organized by phase, of an external penetration test:

Planning

The first step of every penetration test begins with planning. During this phase, the rules of engagement are clearly identified and/or confirmed. These include the type of testing (white, grey or black box), testing goals and the client's preferences about notification and next steps when an exploitable vulnerability is found. Finally, management approval to begin testing is documented via a waiver and network information is shared as determined by the type of testing.

Discovery

External Penetration Testing Discovery involves both Passive and Active Information Gathering:

Passive Information Gathering

While performing reconnaissance of targets in scope, we search for publicly available information using sources such as:

- Whois
- Client website(s)
- Internet Foot Printing – email addresses, usernames, social networks
- Domain Name System records
- Any other publicly facing systems
- Other publicly available information

Active Information Gathering

The Active Information Gathering Phase is where the public facing systems for North Florida College will be tested using various manual methods and commercial scanning tools which will form the foundation for the attack phase. During the active information gather phase, SCA will perform discovery and probing of targets in scope with the following technical activities:

- Port scanning
- OS fingerprinting
- Service enumeration

- Identifying misconfigurations
- Vulnerability analysis (manual testing and commercial tools)
- Validation of discovered vulnerabilities

Attack - Exploitation

The Attack phase includes attempts to exploit found vulnerabilities to gain system access and/or sensitive information. Various techniques will be used including but not limited to manual techniques and automated tools. SCA will take precautions against disruption including a pre-assessment call in the Planning phase to clearly identify expectations, rules of engagement and the identification of systems to exclude from testing. During the pre-assessment call, the client also reserves the right to require approval of any attempted exploitation of systems/services prior to any attempts by SCA personnel. Any critical vulnerabilities are immediately brought to your attention, so they may be remediated.

Should SCA encounter any web applications during the course of external penetration testing, we will treat them as any other IP and test accordingly.

For those who want to test in-house developed web applications or 3rd party developed web applications using methodology that mimics malicious actors, our Web Application Penetration Test is quoted as a separate service upon request.

Reporting

Upon completion, SCA will summarize the penetration testing results for each vulnerability with any information exploited, potential disruptions that could be executed and any remediation or mitigation techniques suggested. Information in this analysis includes:

- Open ports and service information
- Discovered vulnerabilities
- Methodologies used in identifying vulnerabilities
- Exploits attempted
- Exploits successfully executed
- Methodologies used in exploiting vulnerabilities
- Corrective/Remediation advice

Remediation Validation

At the client's option and after a reasonable time for remediation, normally 30 days, SCA will re-test the target IPs to validate remediation efforts. Taking longer time to remediate can potentially allow a malicious actor to exploit weaknesses to gain system access. Re-testing to validate remediation follows our same robust, predominantly manual hands-on keyboard methodology and is not just a scan. Periodic scans after the penetration test are an important component of a prudent vulnerability management program. SCA will quote vulnerability scans upon client request.

Because the amount of remediation and re-testing needed is unknown until the completion of the initial penetration test, remediation validation re-testing is quoted at an hourly rate and will be invoiced for the actual time used.

Deliverables

SCA provides custom reports for each project phase. The External Network Penetration Test reports are separate documents. The reports will reflect individual sections, highlighting each unique assessment focus and offer specific vulnerability findings, prioritization, recommendations and remediation advice. SCA allows for management comment columns, per request.

The reports are segmented and presented as follows:

- Table of Content
- Purpose
- Executive Summary-high level review of process and findings
- Vulnerability Classifications – identifies how each classification level, severe, high, medium, and low are defined.
- Approach and Methodology – explanation of various phases of the engagement.
- Assessment results- segmented by examined area
- Observations- with risk, background, and recommendations.
- Column for client response to findings

Penetration Testing draft reports are delivered within 30 days of completion of testing. North Florida College will be notified immediately of all critical findings during penetration testing so that they can be remediated. North Florida College will have the opportunity to review the draft report with the SCA analyst. If Remediation Validation Testing is not selected, the draft report will be marked as final.

If Remediation Validation Testing is selected, a window of 30 days to remediate will be provided before we re-test. Upon completion of re-testing, a final report will be delivered.

Project Management Approach

SCA has a history of working closely with clients. Assignments are much more fruitful when a relationship is developed from both standpoints. A typical assignment will begin with a conference call to introduce key personnel. Client preferences, expectations and timelines are identified. SCA intent is not to undermine your current efforts, but rather to work with you in an upfront manner to validate and document your posture. Interactive sessions will present alternatives to your practices and allow for consensus on remediation and course. North Florida College will always be aware of pending report content in advance, thus no surprises. SCA will honor North Florida College preferences for each project phase.

Complementing Services

Security Compliance Associates delivers many more world-class information security and compliance services. North Florida College may wish to consider the following either now or in the future:

- Regulatory Gap Analysis
- NIST Cybersecurity Framework Assessment
- NIST Privacy Framework Assessment
- Cybersecurity Risk Assessment
- Controls Review (CIS, ISO27002, NIST 800-171, NIST 800-53)
- ISO27001 Readiness Assessment
- PCI Readiness Assessment
- Application Assessments and Penetration Testing
- Social Engineering
- Employee Information Security Awareness Training
- 3rd Party Due-Diligence
- Information Security Policy Program
- DR/BC Plan Program
- Incident Response Program
- Centurion ESO (Executive Security Officer) Services

SCA now offers a dynamic, user-friendly email phishing and cybersecurity awareness training platform from Phished!

Detailed and Annualized Fees

North Florida College

Description	Annual Qty.	Unit Cost	Total
External Network Penetration Testing White Box, 25 IPs, 16 Hours	1	$3,600	**$3,600**
Total Project Fees:			**$3,600**
Optional Services			
Remediation Validation Re-Testing Network and Application	TBD	$250/hr.	TBD
Fees are valid for sixty (60) days from the date of this proposal			

Terms:

1. 50% of the Total Project Fees ($1,800) is due on the "Effective Date" of Master Services Agreement.
2. Balance ($1,800) due six months after "Effective Date" or at project completion, whichever occurs first.
3. Travel, if needed, is invoiced separately at actual cost.
4. All invoices are due upon receipt.
5. Remittance by ACH (preferred), Check or Credit Card (4% Fee for Credit Card).

North Florida College may elect a multiple year Agreement for annual service delivery. In consideration for a multiple year Agreement, SCA will maintain the above fees for the duration of the Agreement, up to 3 years, unless there are changes to the project scope or economic conditions that require a fee adjustment.

Multi-year agreements are invoiced bi-annually in 50% installments with adjustment to the Terms as follows:

Total Annual Fees will be invoiced in two 50% bi-annual installments of ($1,800) each beginning on the "Effective Date" and for the duration of the Multi-Year Master Services Agreement.

Project Team Staffing Leaders

SCA's hiring policy prohibits employing individuals with felony convictions, and no current SCA employee has been convicted of a felony. Employee eligibility to work in the United States is verified through e-Verify at the time of hire. SCA also maintains multi-million-dollar errors and omissions insurance coverage. The table below lists the team members who will be assigned to this project based on availability and need. We have provided a brief overview of each member's skills and how they relate to the project's scope outlined in this proposal. Upon contract award and depending on availability, more detailed candidate resumes can be provided upon request.

POSITION	CANDIDATE SUMMARY	CREDENTIALS
CIO	**Jim Catrett, MSIT**, started with SCA as a Senior Analyst in Information Security Compliance, with an educational background in Information Assurance and Security. Now serving as a CIO, Jim oversees SCA's compliance service portfolio. He has conducted over 150 information security risk assessments and developed numerous policy and procedure review programs. Jim is committed to helping organizations surpass compliance and regulatory standards in information security. He holds a Master of Science in Information Technology, specializing in Information Assurance and Security, with a focus on policy and procedure development and business continuity planning development.	MSIT, CCSFP, CHQP, Cyber AB-RP
CISO	**Maja Bobic, CISSP, CISA, CCSFP**, **CHQP** is a much sought after executive in the Information Security, Compliance and corporate governance space. She has advised multi-billion dollar financial institutions, State Government Agencies, Large Health Care Operations and many other organizations where cybersecurity is a mission critical part of their infrastructure. Maja is currently serving as Chief Information Security Officer at SCA where she oversees a team of cybersecurtiy analysts that perform cybersecurity assessment and advisory services for companies seeking to improve their cybersecurity posture as well as conform to compliance regulations such as GLBA, HIPAA, CMMC, and other mandates. Maja is also Vice President of ISSA Tampa Bay Chapter and an active member of InfraGard. Maja holds a Bachelor degree in MIS with a concentration in Information Security. With over 15 years of experience in the field and as a corporate leader, Maja brings real world expertise from behind the scenes of hundreds of organizations as well as direct experience as a CISO managing the current threat environment by leveraging people, technology and best practices	CISSP, CISA CCSFP, CHQP

POSITION	CANDIDATE SUMMARY	CREDENTIALS
Senior Penetration Tester	**Ben Johnson, CISSP, GMOB, GWAPT,** brings over a decade of experience in web and mobile application penetration testing and vulnerability assessments. His proficiency extends to conducting mobile application code reviews and application code reviews. Additionally, he possesses skills in both internal and external network penetration testing as well as desktop applications. Moreover, he is adept at conducting penetration tests specifically for iPhone and Android mobile applications. Able to leverage impressive grasp of cyber security best practices and analytical capabilities that allows collaboration effectively within a team environment and create solutions unique to individual Pasco Countyneeds and can relay technical knowledge to wide array of audience including non-technical board members. Graduated from the University of South Florida in 09' with a bachelor's degree in criminology. Currently holds; CISSP, GMOB and GWAPT certifications.	CISSP, GMOB, GWAPT