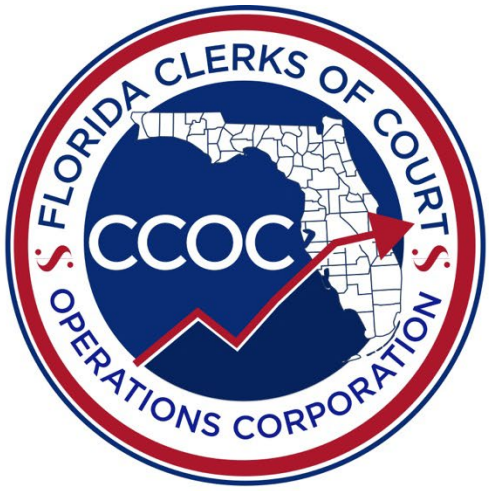

EXECUTIVE COMMITTEE MEETING

March 6, 2024

EXECUTIVE COMMITTEE MEETING

March 6 , 2024
Meeting: 4:00 PM, Eastern

Microsoft Teams meeting

Join on your computer, mobile app or room device

Click here to join the meeting

Meeting ID: 241 669 667 633
Passcode: TnWL4u

Call to Order.....Hon. Stacy Butterfield
Roll Call.....Hon. Laura Roth
1) Introduction and Agenda Approval.....Hon. Stacy Butterfield
2) Review of Contract with CPA for Internal Audit Services.....Hon. Laura Roth
3) Review of Contract for IT Services Review.....John Dew
4) Other Business.....Hon. Stacy Butterfield

DRAFT PROFESSIONAL SERVICES AGREEMENT

This Agreement made this __ day of March 2024, between the Florida Clerks of Court Operations Corporation (hereinafter the "Corporation"), having its principal place of business at 2560-102 Barrington Circle, Tallahassee, Florida 32308 and Thomson Brock Luger & Company (hereinafter "Vendor"), 3375-G Capital Circle NE, Tallahassee, Florida 32308.

WHEREAS, the Legislature created the Florida Clerks of Court Operations Corporation in Section 28.35, F.S.; and

WHEREAS, the Corporation is charged under Section 28.35, F.S., and other relevant Florida Statutes with certain duties and responsibilities which include budget planning, budget review, and the development and certification of a uniform system of performance measures, and

WHEREAS, the Corporation has determined that in order to meet its statutory obligations, certain professional services will be required; and

WHEREAS, the Corporation has determined that the Vendor has the experience of financial and accounting services to meet the Corporation's needs and requirements in a timely and professional manner; and

WHEREAS, the Corporation wishes to contract with Vendor, on a non-exclusive basis, for certain services as hereafter defined and the Vendor is willing to enter into such an Agreement to provide such services to the Corporation. Therefore,

IN CONSIDERATION of the aforementioned representations, it is hereby agreed as follows:

SECTION 1: SERVICES

1.1 The Corporation hereby retains Vendor to furnish certain services, information, and items as provided below, but reserves the right to select additional contractors.

1.2 Assignments shall be directed by the Executive Director or the Contract Manager.

1.3 Services that may be provided by Vendor to the Corporation pursuant to this Agreement and hereinafter defined shall include specific areas of:

A. Financial and Accounting Services

1.4 Services to be provided by Vendor as delineated and hereinafter defined shall be provided as desired and to the extent determined by the Corporation, as directed.

1.5 Services to be provided by Vendor shall be performed and delivered at the Corporation principal place of business unless provided otherwise.

SECTION 2: DEFINITION AND SCOPE OF SERVICES

Services provided by Vendor pursuant to this Agreement shall be as defined below within the scope and tasks as established.

2.1 Provide financial and accounting assistance to the CCOC staff with reconciliation of bank accounts, payment of payroll taxes and liabilities, and submission of reports.

2.2 Provide assistance in tracking and auditing CCOC's fixed assets.

2.3 Ensure compliance with established internal control policies and procedures by examining records, reports, operating practices, and documentation.

2.4 Assist in providing financial data where needed to respond to auditor findings and recommendations.

2.5 Assist CCOC staff with quality control by reviewing work papers, reports, and charts developed by CCOC staff.

SECTION 3: COSTS

3.1 Rate of Payment

The Corporation's performance and obligation to pay under this contract is contingent upon an annual appropriation by the State of Florida Legislature. Payment for production labor by the Corporation to the Vendor shall be based on the hourly production rate of $105 per hour. Total contract costs not to exceed $28,350. Said rates encompass all employee related expenses such as federal taxes, insurances, retirement, and other federal and/or state required costs and Vendor's overhead related expenses.

3.2 Direct Costs

The Corporation shall reimburse the Vendor for direct costs incurred by Vendor in providing services under this Agreement. Such costs shall include postage, telephone, travel/per diem (subject to state policy and Section 112.061, F.S.), and material/supplies.

3.3 Invoices

The Vendor shall invoice the Corporation upon acceptance of a deliverable by the Corporation, or where appropriate, by the fifteenth of each calendar month for the costs for services rendered by Vendor hereunder for the previous calendar month. Such invoice shall identify the services performed, the dates of such service, Vendor's employee(s) performing service. Direct expense reimbursements, included on invoice shall be supported by appropriate documentation. Invoices are to be provided to the CCOC Executive Director by the 15 of the following month that the work was conducted. Invoices received more than thirty (30) days past the due date are subject to a reduction of payment by 2% per month for each month it is past due. The Corporation shall pay such invoices within thirty (30) days of receipt.

All invoices of Vendor shall be subject to approval of the Executive Director. The Corporation shall pay such invoices within thirty (30) days of receipt, subject to availability of funds.

Upon termination of the contract, the Corporation shall provide payment to the Vendor for approved costs incurred up to the date of termination

SECTION 4: TERM OF AGREEMENT

4.1 Term

This Agreement shall be effective upon the later of the dates signed by the parties and continuing until the Agreement is terminated or canceled under provisions of the Agreement, but no later than December 31, 2024.

4.2 Termination Limitations

This Agreement shall only be terminated or canceled as provided under the provisions herein.

4.3 Termination

Either party may terminate this Agreement for convenience upon providing fifteen (15) days Termination Notice to the other party in writing.

4.4 Mutual Rescission

The parties may mutually agree in writing to terminate this Agreement without further notice.

4.5 Cancellation

If either the Corporation or the Vendor violates its obligations under this Agreement, the other party may cancel this Agreement by sending Cancellation Notice describing the noncompliance to the other party. Upon receiving Cancellation Notice, the noncompliant party shall have ten (10) business days from the date of such notice to cure any such noncompliance. If such noncompliance is not cured within the required ten (10) business days, the other party shall have the right to cancel this Agreement as of the eleventh day after the date of the Cancellation Notice.

4.6 Cancellation Without Notice

Notwithstanding other provisions herein, either party may cancel this Agreement without notice upon the earliest to occur of the following events:

(a) Fraud or Dishonesty: The Corporation or the Vendor commits an act of fraud or dishonesty pursuant to the provisions of this Agreement;

(b) Failure to Perform: The Corporation or the Vendor fails to perform pursuant to the provisions of this Agreement;

(c) Felony Conviction: The Corporation or the Vendor is convicted of a felony.

SECTION 5: RESPONSIBILITIES OF VENDOR

5.1 Vendor fully understands and agrees that there shall be no reimbursement of funds by the Corporation for any obligation or expenditure made prior to the execution of this Agreement.

5.2 All direction for services shall be either verbally or in writing by the Executive Director or the Executive Director's designee.

5.3 All services described in the Agreement shall be performed by and/or under the direct supervision of John K. Kirk, (telephone number 850-385-7444), or another person of similar experience designated by Vendor and approved, in writing, by the Corporation's Contract Manager. For the purposes of this Agreement, such approved person shall be considered the Vendor.

5.4 To the extent required by law, the Vendor shall maintain, during the life of this Agreement, Workers' Compensation insurance for all of its employees connected with any work related to this Agreement. Such insurance coverage shall comply fully with the Florida Workers' Compensation law. In case any class of employees engaged in hazardous work under this Agreement are not protected under Workers' Compensation statutes.

5.5 All notes and work product associated with this Agreement shall be open for review by the Corporation's Contract Manager by request in writing, the vendor shall have 10 days to produce the items requested.

5.6 Vendor shall be responsible for all work performed under the terms of this Agreement. It is agreed that none of the services performed under this Agreement shall be subcontracted to any individual or firm without the prior written consent of the Corporation's Contract Manager. It is understood that these subcontractors shall only work in their area of expertise. The Corporation reserves the right to require the Vendor to remove a subcontractor if, during the term of this Agreement, any work performance of the subcontractor deemed unsatisfactory by the Corporation.

5.7 Vendor shall retain financial records, supporting documentation, statistical, and all other records pertinent to this Agreement for a period of three (3) years after final payment is made, except that such records shall be further retained until final resolution of any matters resulting from any litigation, claim, or audit that started prior to the expiration of the retention period. The retention period commences from the date of the submission of the final expenditure report. The records and documents shall be made available to the Corporation upon request. Vendor agrees that all physical records referenced in this paragraph, and any other records relative to this Agreement, shall be maintained by the Vendor at a location within the state of Florida.

5.9 All records of the Vendor with respect to this Agreement shall be public record and shall be treated in the same manner as other public records are treated under general law.

SECTION 6: MISCELLANEOUS

6.1 Confidentiality

Expect as provided above, the Vendor recognizes and acknowledges that the functions the Corporation performs may provide access to matters, which are, by Florida Statute, confidential (hereinafter referred to as "Confidential Information") and that any unauthorized disclosure of same would cause irreparable damage. Vendor agrees that, except as directed by the Corporation, it will not at any time during or after the term of the Agreement disclose any Confidential Information to any person whatsoever. Accordingly, the Corporation may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies available by law, which may be available. The Vendor hereby recognizes that disclosure of Confidential Information would be a breach of this Agreement however; any information made public by Florida law shall be exempt from this provision.

6.2 Relationship of Parties

Notwithstanding any other provisions contained herein, it is expressly agreed that the Vendor is an independent contractor in the performance of each and every part of this Agreement. As such, the Vendor is solely liable for all acts and omissions of itself, its officers, its employees, its agents, and subcontractors, for all labor and expenses in the performance of services, unless otherwise specified in this Agreement. It is expressly agreed that the Vendor, its officers, employees, agents, and subcontractors shall act in an independent capacity and not as officers, employees, or agents of the Corporation in the performance of services under this Agreement.

It is further expressly agreed that this Agreement shall not be construed as a partnership or joint venture between the Corporation and the Vendor. Vender shall have no authority to bind the Corporation for the performance of any contract or otherwise obligate the Corporation, except as specifically set forth in this Agreement.

6.3 Assurances

The Corporation and Vender represent and warrant that all representations, warranties, recitals, statements, and information provided under this Agreement are true, correct and accurate as of the date of this Agreement.

6.4 Conflict of Interest

The Vendor covenants that it presently has no interest and shall not acquire any interest which would conflict in any manner or degree with the performance of the services required.

This Agreement is not intended, nor shall it be construed as granting any rights, privileges, or interest in any third party without mutual written Agreement of the parties hereto.

6.5 Discrimination

No person, on the grounds of race, creed, color, national origin, age, sex, or disability shall be excluded from participation in, be denied the proceeds or benefits of, or be otherwise subjected to discrimination in performance of this Agreement.

6.6 Entire Agreement

This Agreement contains the entire understanding of the parties relating to the Services and supersedes all previous verbal and written Agreements relating to the Services.

6.7 Severability

If a provision of this Agreement is rendered invalid the remaining provisions shall remain in full force and effect.

6.8 Captions

The headings and captions of this Agreement are inserted for convenience of reference and do not define, limit, or describe the scope or intent of this Agreement or any particular section, paragraph, or provision.

6.9 Counterparts

This Agreement may be executed in multiple counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

6.10 Governing Law

This Agreement shall be governed by the laws of the State of Florida and venue shall be Leon County, Florida.

6.11 Notice

All communications shall be in writing. Notices shall be delivered by Certified or Registered Mail - Return Receipt Requested - or by hand to the address set forth below for each party to this Agreement. Notice shall be deemed given on the date of receipt, as evidenced in the case of Certified or Registered Mail by Return Receipt.

CORPORATION	Vendor
John Dew	John K. Kirk, CPA
Executive Director	Thomson Brock Luger & Co.
Clerks of Court Operations Corporation	3375-G Capital Circle NE
2560-102 Barrington Circle	Tallahassee, FL 32308
Tallahassee, Florida 32308	

6.12 Pronouns/Gender

Pronouns and nouns shall refer to the masculine, feminine, singular or plural, as the context shall require.

6.13 Equitable Remedies

The parties hereby acknowledge that damages at law may be an inadequate remedy to the parties. In addition to other rights, which may be available, the parties shall have the right of specific performance, injunction or other equitable remedy in the event of a breach or threatened breach of this Agreement by the other party.

6.14 Litigation Expenses

In the event of litigation or arbitration arising out of this Agreement, the prevailing party shall be entitled to recover its responsible and necessary attorneys' fees and costs.

6.15 Waiver

Waiver of any breach of this Agreement shall not constitute a waiver of any other breach. All remedies under this Agreement are in addition to equitable remedies and remedies provided by law, and are cumulative. Failure to enforce any provision of this Agreement shall not constitute a waiver or create an estoppel from enforcing such provision.

6.16 Assignments

Any and all assignments of rights hereunder by the Corporation and the Vendor shall be void.

6.17 Public Announcements

All public announcements of the relationship of the Corporation and Association under this Agreement shall be subject to the prior written approval of the Corporation.

6.18 Arbitration

Any controversy or claim arising out of or relating to this Agreement, or breach thereof, that cannot be otherwise resolved, shall be settled by arbitration in accordance with the Arbitration Rules of the American Arbitration Association ("Rules of the AAA"), as amended and in effect on the date of service of the demand for arbitration. Any award by the arbitrator shall specify which party is to be deemed the prevailing party. The AAA's and arbitrator's expenses and fees, together with other arbitration expenses including reasonable attorney's fees of the prevailing party, shall be paid for by the non-prevailing party or reimbursed to the prevailing party if advanced by the prevailing party. Judgment, upon the award rendered by the arbitrators, may be vacated by a court of competent jurisdiction in Leon County, Florida. Each party shall have the right of discovery as set forth in the Florida Rules of Civil Procedure.

6.19 No Minimum Level of Work

No minimum level of work is guaranteed as a result of this Agreement. This Agreement is not intended to be a sole source contract or an exclusive contract.

6.20 Fraud Policy

Pursuant to F.S. 112.311, the Corporation and the Vendor acknowledge the following Fraud Policy of the Corporation exists to guard against fraudulent, unethical, and dishonest acts and identify responsibilities for preventing, detecting, reporting, and investigating such. Sections 6.21-6.23 below outline the Fraud Policy and Procedures of the Corporation (therein "CCOC").

6.21 Background/Objective

The CCOC recognizes the importance of protecting the organization, its operations, its employees and its assets against financial risks, operational breaches, and unethical activities. Therefore, it is incumbent upon

CCOC's Executive Director to institute and clearly communicate the fraud prevention policy to employees, both internal and external customers, vendors, and partners.

The CCOC is committed to the highest standards of moral and ethical behavior. Breaches of these standards, especially through acts involving fraudulent, unethical, and other dishonest behavior, are not only costly, but they erode the public's trust and confidence in the integrity of the agency. By issuing this formal policy statement, the CCOC hereby reaffirms its longstanding duty and responsibility to aggressively combat such behavior.

The CCOC recognizes a zero-tolerance policy regarding fraud and corruption. All matters raised by any source will be taken seriously and properly investigated. This policy covers all CCOC employees and Council Members. Additionally, this policy covers consultants, vendors, contractors, outside agency, or a person doing business with the agency or in any other relationship with the agency to the extent that the CCOC resources are involved or impacted.

An employee who, in good faith, reports wrongful activity meeting the provisions of s. 112.3187, F.S. (Whistle-blower's Act), is protected against retaliation for making such a report. The law also provides for the individual's identity to remain confidential. Regardless as to whether or not the provisions of the Whistle-blower's Act are met, it is a violation of this policy for anyone to retaliate against an employee for reporting, in good faith, allegations of wrongdoing, or participating in the investigation of such.

The CCOC's policy is to promote consistent, legal, and ethical organizational behavior by:

- assigning responsibility for reporting fraud, theft, waste, or abuse;
- institute preventive measures designed to deter these activities or make them easier to detect;
- providing guidelines for reporting and investigating suspected fraudulent behavior;
- requiring each employee to attend fraud awareness training;

Failure to comply with this policy subjects an employee (including management) to disciplinary action, including immediate termination. Failure to comply by a consultant, vendor, contractor, outside agency, or a person doing business with the agency or in any other relationship with the agency could result in cancellation of the business or other relationship between the entity and the CCOC.

For purposes of this policy only the term ***fraud*** or ***fraudulent*** includes theft, waste, and abuse as defined below. The term ***employee*** also includes employees in management positions. The term ***management*** includes council members, managers, assistant managers, supervisors, and any other employee who has authority to sign another employee's performance evaluation and/or timesheet.

Definitions and Examples of Fraud, Waste, Abuse and Corruption

Fraud is defined as an intentional deception designed to obtain a benefit or advantage or to cause some benefit that is due to be denied. Fraud generally involves a willful or deliberate act or omission with the intention of obtaining an unauthorized benefit, service, property, or something of value by deception, misrepresentation, or other unethical or unlawful means. Fraud can be committed through many methods, including mail, wire, telephone, and the Internet. Fraudulent, unethical, and other dishonest acts may include, but are not limited to, the following:

- Forgery or alteration of a check, bank draft, any other financial document, or computer records;
- Falsification or misrepresentation of reports to management and external agencies, including time sheets, official travel claims for reimbursement, or other expense reimbursement reports;
- Knowingly authorizing or receiving payment for time not worked;
- Misappropriation of funds, securities, supplies, or other assets;
- Impropriety in the handling or reporting of money or financial transactions;
- Engaging in unauthorized activities that result in a conflict of interest;

- Disclosing confidential or proprietary information to unauthorized individuals;
- Removal of agency property, records, or other assets from the premises without supervisory approval;
- Unauthorized use or destruction of agency property, records, or other agency assets; and
- Taking and using information or providing the information that would lead to identity theft.
- Theft of cash or fixed assets;
- Failure to account for monies collected;
- Knowingly providing false information on job applications and requests for funding;

6.22 Investigate

Upon reviewing allegations of fraudulent, unethical, or dishonest acts, if the Executive Director determines an investigation is warranted, he/she shall appoint a qualified individual or entity to investigate the reported activity after consulting with the General Counsel. In those instances where the investigation by the Executive Director–Appointee indicates potential criminal activity, the investigation shall immediately be turned over to the Florida Department of Law Enforcement and the State Attorney's Office.

During the investigation, the Constitutional rights of all persons are to be observed. The accused will be afforded the opportunity to respond to the allegations or matters being investigated. The rights of the accused will be safeguarded throughout the investigation.

Pursuant to this policy, all employees are to cooperate fully with those performing an investigation. An employee who does not fully cooperate with an authorized investigation may be disciplined, up to and including termination of employment. An employee may be required to answer any questions that are within the scope of the employee's employment, whether such questions are asked in an investigation conducted by the Executive Director Appointee or Human Resources.

The investigation shall be completed expeditiously and in accordance with established procedures. The results of the investigation conducted by the Executive Director Appointee shall be communicated, either orally or in writing, to the Executive Director.

Allegations or matters of conduct deemed outside the scope of this policy, such as supervisory or personnel-related issues, may be referred to the respective area of management or the Human Resources Section for review and appropriate action.

6.23 Actions

Employees, consultants, vendors, contractors, outside agency, or a person doing business with the agency or in any other relationship with the agency to the extent that the CCOC resources are involved or impacted is determined to have participated in fraudulent, unethical, or dishonest acts will be subject to disciplinary action in accordance with personnel policies and rules. Criminal, civil, and/or other administrative actions may also be taken against employees who are found to have participated in unlawful acts. Criminal action falls within the sole purview of local, state, or federal law enforcement, as well as prosecuting and judicial authorities. In those instances where disciplinary and/or other administrative action is warranted, the Human Resources Section, or other appropriate office, shall be consulted prior to taking such actions.

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto as of the Effective Date of March ___, 2024.

Florida Court Clerk of Court Operations Corporation	**John K. Kirk, CPA**
_____	_____
Signature	Signature
Stacy Butterfield Chair	John K. Kirk, CPA Thomson Brock Luger & Company
_____	_____
Date	Date

Erikson Security

Security Assessment
Statement of Work
PROPOSAL

Florida Clerks of Court
Operations Corporation

February 27, 2024

Change Revision

Version	Date	Author	Description
1.0	2/27/2024	David Blake	Initial Proposal

Contacts

Name	Title	Phone	Email
David Blake	Consultant	336-671-7317	dblake@eriksonsecurity.com

Table of Contents

Executive Summary

Project Overview

This Statement of Work (SoW) outlines the security assessment services to be provided for Florida Clerks of Court Operations Corporation. The objective is to identify vulnerabilities, potential security weaknesses, and provide recommendations for strengthening the security posture of the organization's IT environment.

Objectives

- To identify and prioritize security vulnerabilities in the client's external and internal network infrastructure.
- To assess the security of web applications against industry best practices and known vulnerabilities.
- To review the configuration and security posture of Azure and Microsoft 365 environments.

Scope

Note: There are no known daily time restrictions on when testing can be performed.

External Penetration Test

- One (1) external IP address

Web Application Penetration Test

- Two (2) publicly available web applications
  - Option 1
    - Unauthenticated testing only of both applications
  - Option 2
    - Unauthenticated and authenticated testing of both applications

Internal Vulnerability Assessment

- Less than 20 internal systems
- Scanning will be performed from a system inside the network
- Appropriate administrative credentials to be provided for each in-scope system

Internal Penetration Test

- Less than 20 internal systems and users
- One (1) Active Directory domain
- Testing will be performed from a system inside the network based on starting scenario

Azure Security Review

- One (1) Azure tenant
- Azure subscriptions are out-of-scope

Microsoft 365 Security Review

- One (1) Microsoft 365 billing account

Remediation Testing and Review

- Retest and review of discovered issues that were stated as remediated
    - One (1) remediation assessment
        - Retest to be performed within 120 days of initial deliverable(s) release

Methodology

This methodology section provides a structured approach to each phase of the security assessment, ensuring comprehensive coverage of the organization's security posture.

Initial Assessment

External Penetration Test

- **Reconnaissance:** Collect publicly available information to identify potential targets and understand the external digital footprint.
- **Scanning:** Use automated tools to scan for open ports, services, and vulnerabilities on external-facing systems.
- **Vulnerability Assessment:** Analyze the findings from the scanning phase to identify exploitable vulnerabilities.
- **Exploitation:** Attempt to exploit identified vulnerabilities to gain unauthorized access or extract data, simulating an attacker's approach.

Internal Vulnerability Assessment

- **Network Scanning:** Scan the internal network for devices, services, and vulnerabilities using a range of automated tools.
- **Vulnerability Identification:** Assess the scan results to identify vulnerabilities, focusing on severity and potential impact.
- **Risk Analysis:** Evaluate the risks associated with identified vulnerabilities in the context of the organization's environment.

Internal Penetration Test

- Pre-Engagement: Define the scope and rules of engagement with stakeholders to ensure a clear understanding and minimize operational impact.
- **Initial Exploitation:** Utilize identified vulnerabilities from the internal vulnerability assessment to gain initial access to systems.
- **Lateral Movement:** Attempt to move across the network to access critical systems and data, emulating a malicious insider or a compromised account.
- **Persistence and Escalation:** Test the ability to maintain access and escalate privileges within the network.

Web Application Penetration Test

- **Application Mapping:** Perform a thorough examination of the web application to understand its structure, functionalities, and entry points.
- **Vulnerability Scanning:** Use automated tools and manual techniques to identify security weaknesses and technical vulnerabilities.

- **Exploitation:** Attempt to exploit identified vulnerabilities, focusing on injection flaws, broken authentication, sensitive data exposure, and cross-site scripting (XSS).
- **Business Logic Testing:** Test the application's business logic for flaws that could be exploited in a real-world attack.

Azure Security Review

- **Configuration Review:** Examine Azure environments against best practices for security, compliance, and performance.
- **Identity and Access Management (IAM) Review:** Assess the policies and controls around user identities, permissions, and roles.
- **Resource and Network Security:** Evaluate the security configuration of Azure resources and network architecture.
- **Data Protection and Compliance:** Review data storage, encryption, and compliance settings against regulatory requirements.

Microsoft 365 Security Review

- **Configuration and Compliance Check:** Review Microsoft 365 tenant configurations, including security and compliance settings.
- **Email Security:** Assess email protection mechanisms, including anti-phishing, anti-malware, and spam filters.
- **Data Governance:** Evaluate data loss prevention (DLP), encryption, and information protection policies.
- **Identity and Access Management (IAM):** Review the implementation of conditional access, multi-factor authentication (MFA), and role-based access control (RBAC).

Remediation Testing

After the completion of the initial security assessment phases and the implementation of the recommended remediations by the client, a follow-up assessment is conducted to validate the effectiveness of the remediation efforts and to ensure that previously identified vulnerabilities have been adequately addressed. This phase is critical for closing the loop on the security assessment process and ensuring ongoing improvements to the security posture.

- **Remediation Plan Review:** Begin with a review of the remediation actions taken by the client in response to the initial assessment findings. This involves discussions with relevant teams to understand the scope and depth of the remediation efforts.
- **Verification Scans:** Conduct targeted scans and tests focusing on the areas where vulnerabilities were previously identified. This includes using automated tools and manual testing techniques to verify that vulnerabilities have been resolved and that no new vulnerabilities have been introduced during the remediation process.
- **Remediation Validation Report:** Produce a detailed report that outlines the findings of the remediation assessment, including evidence of remediation, any remaining vulnerabilities, and recommendations for further action if necessary. This report serves as a record of the progress made in enhancing the organization's security posture.

- **Feedback and Improvement Session:** Organize a session with key stakeholders to discuss the findings of the remediation assessment, provide feedback on the remediation efforts, and discuss strategies for continuous improvement in security practices.

The Remediation Assessment methodology is designed to ensure that remediation efforts are thoroughly validated, providing organizations with confidence in their security measures and a clear path toward continuous security improvement. This comprehensive approach helps to ensure that vulnerabilities are not only identified and fixed but that the fixes are effective and sustainable over time.

Deliverables

Deliverable	Description
Comprehensive Security Assessment Report	A consolidated report that includes all phases of the security assessment: **External Penetration Test:** Findings, vulnerabilities, test methods, evidence of breaches/exploits, and remediation recommendations **Internal Vulnerability Assessment:** Results of the vulnerability scan, severity of detected vulnerabilities, and corrective actions. **Internal Penetration Test:** Summary of findings, exploited vulnerabilities, impact assessment, and security enhancement recommendations. **Web Application Penetration Test:** Analysis of web application security, vulnerabilities, exploitation attempts, and security recommendations. **Azure Security Review:** Overview of Azure security posture, vulnerabilities, misconfigurations, and cloud security enhancement recommendations. **Microsoft 365 Security Review:** Assessment of Microsoft 365 configurations, security gaps, compliance issues, and security recommendations.
Executive Summary	An integrated high-level summary within the comprehensive report, highlighting key findings, critical vulnerabilities, and prioritized recommendations for executive leadership.
Internal Vulnerability Assessment Findings Spreadsheet	A spreadsheet detailing each identified vulnerability during the internal vulnerability assessment phase, including location, severity, potential impact, and preliminary remediation advice.
Remediation Guidance and Best Practice Advice	Detailed strategies and best practices for remediating identified vulnerabilities, included within the comprehensive report to assist in improving the security posture.
Debriefing Session	A session with key stakeholders to discuss the comprehensive report's findings, clarify any aspects, and strategize for remediation and improvement steps.

Pricing

Cost and Hours Breakdown

Option 1 – Unauthenticated Web Application Testing

Phase	Estimated Hours	Cost per Hour	Phase Cost	w/ Remediation Testing
External Penetration Test	5	$150	$ 750.00	$ 900.00
Internal Vulnerability Assessment	15	$150	$2,250.00	$2,700.00
Internal Penetration Test	30	$150	$4,500.00	$5,400.00
Web Application Penetration Test (Two Apps)	30	$150	$4,500.00	$5,400.00
Azure Security Review	20	$150	$3,000.00	$3,600.00
Microsoft 365 Security Review	20	$150	$3,000.00	$3,600.00
Total	**120**		**$18,000.00**	**$21,600.00**

Option 2 – Authenticated Web Application Testing

Phase	Estimated Hours	Cost per Hour	Phase Cost	w/ Remediation Testing
External Penetration Test	5	$150	$ 750.00	$ 900.00
Internal Vulnerability Assessment	15	$150	$2,250.00	$2,700.00
Internal Penetration Test	30	$150	$4,500.00	$5,400.00
Web Application Penetration Test (Two Apps)	80	$150	$12,000.00	$14,400.00
Azure Security Review	20	$150	$3,000.00	$3,600.00
Microsoft 365 Security Review	20	$150	$3,000.00	$3,600.00
Total	**170**		**$25,500.00**	**$30,600.00**

Note: Costs and hours are estimates and may be subject to adjustments based on the specific needs and complexity of the client's environment. Phases can be removed or added, based on client needs.

Timeline

The total assessment is scheduled over a 7-week period, subject to the complexity and size of the environment.

- Week 1: External Penetration Test
- Week 1-2: Internal Vulnerability Assessment
- Week 3: Internal Penetration Test

- Week 4-5: Web Application Penetration Test
- Week 6: Azure Security Review
- Week 7: Microsoft 365 Security Review

Location

All work will be performed remotely via public internet and/or access methods provided by the organization.

Terms and Conditions

The following terms and conditions shall apply for this, and all revisions, Statement of Work (SoW) between Erikson Security, LLC (SERVICE PROVIDER) and Florida Clerks of Court Operations Corporation (CLIENT).

Intellectual Property

- Ownership: All methodologies, tools, and software used in the execution of this SoW remain the property of SERVICE PROVIDER. Any modifications or improvements made during the engagement will also be the property of SERVICE PROVIDER.
- Client Data: All data, information, and materials provided by CLIENT for the purpose of this engagement remain the intellectual property of CLIENT. SERVICE PROVIDER acknowledges that no ownership of CLIENT's intellectual property rights is transferred as a part of this agreement.

Confidentiality

- Agreement: Both parties agree to maintain the confidentiality of all information shared during and after the completion of the engagement. Confidential information shall not be disclosed to third parties without prior written consent from the disclosing party.
- Security: SERVICE PROVIDER will implement reasonable and appropriate measures to protect the confidentiality and integrity of CLIENT's data.

Limitation of Liability

- Liability Limit: SERVICE PROVIDER's total liability under this SoW for all claims shall not exceed the total amount paid by CLIENT for the services rendered.
- Indirect Damages: In no event will SERVICE PROVIDER be liable for any indirect, incidental, special, or consequential damages arising out of or related to this SoW, regardless of the foreseeability of those damages.

Authorization for Testing

- Consent: CLIENT authorizes SERVICE PROVIDER to perform security assessment activities as outlined in the SoW. This includes access to CLIENT's systems, networks, and data as necessary for the completion of the engagement.
- Legal Compliance: CLIENT confirms that they have the legal authority to engage in these activities and that the testing will not violate any laws or regulations.

Deliverable Acceptance

- Review Period: CLIENT will have a period of 30 business days from the receipt of each deliverable to review and either accept or provide detailed feedback on the deliverable.
- Corrections: Should any deliverables be deemed unsatisfactory, SERVICE PROVIDER agrees to make reasonable corrections at no additional cost to CLIENT, provided the feedback is given within the specified review period.
- Final Acceptance: Deliverables shall be considered accepted if CLIENT does not provide feedback within the review period.

Termination

- Termination for Convenience: Either party may terminate this SoW with 30 days' written notice to the other party.
- Termination for Cause: Either party may terminate this SoW immediately upon written notice if the other party breaches any of its material obligations under this SoW and fails to cure such breach within 30 days from receipt of the breach notice.