ERMProtect
Cybersecurity Solutions

May 13, 2024

STATEMENT OF WORK

Phase One – Digital Forensic Investigation

The purpose of this Statement of Work is to provide a high-level outline of investigative steps and deliverables related to a digital forensic investigation for the City of Doral, based on preliminary discussions with City of Doral procurement and IT officials. Our detailed methodology for this investigation is set out in our response to ITN – 2024-05 dated April 2, 2024. This SOW also sets out our fee schedule.

Case Objectives and Next Steps

Our understanding of the objective of the investigation is have an independent third-party identify users who accessed files on a shared drive utilized by commissioners and their respective legislative aides / chiefs of staff, dating from January 1, 2018, through May 13, 2024. The objective is to identify the usernames, dates, and times of access to shared files of about thirty (30) individuals.

Our investigative steps in Phase One of the investigation will consist of the following:

- ERMProtect personnel will attend separate meetings with four (4) Council Members and the mayor to understand their concerns about access controls and the state of cybersecurity in the city of Doral.
- ERMProtect personnel will send the city of Doral a list of technical requirements and needs to carry out a forensic investigation related to access to shared files. This will include information about servers, logging, and other evidence / data required to carry out the investigation.
- ERMProtect will review any IT Department internal reports related to the access issue and review the adequacy of steps the department took to restrict access.
- ERMProtect personnel will interview city of Doral IT personnel to clarify and ensure our understanding of the technical information provided, along with the IT infrastructure, practices, and procedures in the city of Doral related to access to the shared files. If necessary and possible, ERMProtect may also conduct interviews with past city of Doral IT directors.
- ERMProtect will conduct an independent, forensic analysis and investigation based on the available evidence. ERMProtect will notify the city of any limitations to the investigation related to the availability or unavailability of information.
- ERMProtect will provide the city of Doral with a report and appendices outlining access by username, date, and time to specific shared files, if data is available to provide same. Additionally, ERMProtect will attempt to identify what information was accessed, updated, changed, deleted, moved, or extracted from the systems. The report will include an Executive Summary, with clear, non-technical language.

- Working with the City Attorney, ERMProtect will provide the city of Doral with recommendations for SOPs related to access controls, logging and other practices that preserve the files for the public record, while also ensuring security from improper access.

FEES – FORENSIC INVESTIGATION & TESTIMONY

ERMProtect will charge a blended rate of $250 an hour for forensic work and court testimony, a discounted rate extended to government clients. It is difficult to assess the hours required for a forensic investigation, prior to knowing the evidence available to us for analysis and the IT security policies of the city of Doral. However, based on our experience, we estimate that the forensic phase of this investigation will require from 120 to 160 hours, depending on the availability of evidence.

Every Friday, we will report to the Department of Information Technology with a copy to the Department of Procurement and Asset Management the hours expended so that the city knows where we are on budget and our proposed next steps. Please note that if we require less time for the investigation, we will inform the city as soon as possible. No time will be charged beyond what is absolutely necessary to achieve case objectives.

Agreed:

Silka Gonzalez

Silka González
President, Enterprise Risk Management, Inc.
d/b/a ERMProtect

Date: May 13, 2023

Rey Valdes
City Manager
City of Doral

Date: 6/25/2024

AGREEMENT BETWEEN THE CITY OF DORAL AND ENTERPRISE RISK MANAGEMENT, INC. FOR INDEPENDENT IT SECURITY AUDIT SERVICES

THIS CONTRACTUAL AGREEMENT (hereinafter referred to as the "Agreement") is made this ______day of June, 2024 (the "Effective Date"), by and between the **CITY OF DORAL**, Florida, (hereinafter referred to as "City"), and **ENTERPRISE RISK MANAGEMENT, INC. DBA ERMPROTECT**, a Florida corporation authorized to do business in the State of Florida (hereinafter referred to as "Contractor") whose Federal I.D. # is 65-0827427.

RECITALS

WHEREAS, the City of Doral is in need of a contractor to provide independent information technology auditing services ("Services"); and

WHEREAS, the City issued Invitation to Negotiate No. 2024-05 for the Services (the "ITN"), and upon completion of Procurement staff's review, Contractor was deemed the top ranked proposer; and

WHEREAS, pursuant to Resolution No. 24-122, the City Council awarded the ITN to Contractor in accordance with its proposal, attached hereto as Exhibit "A"; and

WHEREAS, the City wishes to contract with Contractor to provide the desired Services on an as-needed basis pursuant to the terms and conditions contained herein.

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

TERMS

1. **RECITALS.** The Recitals set forth above are hereby incorporated into this Agreement and made a part hereof for reference.

2. **THE CONTRACT DOCUMENTS.** The Contract Documents consist of this Agreement, as well as all Exhibits hereto and the ITN, which terms are specifically incorporated into this Agreement as if set forth in full herein (collectively, hereinafter referred to as the "Contract Documents").

3. **SERVICES.** Contractor shall provide the services pursuant to the terms and conditions set forth in the Contract Documents, as more particularly described in the Contract Documents (hereinafter referred to as "Services"). Each particular assignment authorized under this Contract will be pursuant to a specified agreed-upon scope and the issuance of a Purchase Order by the City.

The Services shall be performed by Contractor to the full satisfaction of the City. Contractor agrees to furnish all labor and material in a good and workmanlike and professional manner to perform Services. Contractor agrees to have a qualified representative to audit and inspect the Services provided on a regular basis to ensure all Services are being performed in accordance with the City's needs and pursuant to the terms of this Agreement and shall report to the City accordingly. Contractor agrees to immediately inform the City via telephone and in writing of any problems that could cause damage to the City's property, improvements and persons. Contractor will require its employees to perform their work in a manner befitting the type and scope of work to be performed. In the event that the Contractor fails to complete the Services pursuant to the terms of this contract and City must undertake the completion of performance of Services, Contractor agrees to indemnify the City for all costs incurred with respect to the completion of those Services and any damages the City may suffer as a result of the Contractor's failure to perform the Services.

4. **TERM.** Subject to the provisions relating to the termination of this Agreement as set forth hereunder, the initial term of this Agreement shall be for a period of one (1) year, beginning on the Effective Date. Prior to, or upon completion of that initial term, the City shall, at its sole and absolute discretion, have the option to renew the contract for two (2) additional one (1) year periods under the same terms and conditions.

Payment will be made only for work completed to the satisfaction of the City. Contractor is to commence performance of work from the date of this Agreement and continue in a diligent manner until completion of the Services. The terms of Sections 8, 18, and 19 entitled "Warranty of Services," "Indemnification and Waiver of Liability," and "Compliance with Law," respectively, shall survive termination of this Agreement.

5. **COMPENSATION.** During the term of this Agreement the City shall pay Contractor for Services at a cost that shall not exceed the hourly rates attached hereto as Exhibit "B" and shall complete the scope subject to the total not-to-exceed amount that will be set forth in the Purchase Order issued for each assignment. Pricing shall remain firm and fixed during the term, including extensions, although Contractor may offer incentive discounts. Payment to Contractor for all charges and tasks under this Agreement shall be in accordance with the Contract Documents and the schedule of charges as reflected in Exhibit "B", under the following conditions:

a. Disbursements. There are no reimbursable expenses associated with this contract except for expenses approved by the City Manager.

b. Payment Schedule. Invoices received from the Contractor pursuant to this Agreement will be reviewed by the initiating City Department and shall comply with Section 3.15 of the ITN. If services have been rendered in conformity with the Agreement, the invoice will be sent to the Finance Department for payment.

c. Availability of Funds. The City's performance and obligation to pay under this Agreement is contingent upon an annual appropriation for its purpose by the City Commission. If the City should not appropriate or otherwise make available funds sufficient to purchase the Services procured pursuant to this Agreement, the City may unilaterally terminate any and all contractual or other obligations herein without any further liability or penalty upon thirty (30) days' notice to Contractor.

Contractor shall make no other charges to the City for supplies, labor, taxes, licenses, permits, overhead or any other expenses or costs unless any such expense or cost is incurred by Contractor with the prior written approval of the City. If the City disputes any charges on the invoices, it may make payment of the uncontested amounts and withhold payment on the contested amounts until they are resolved by agreement with Contractor. Contractor shall not pledge the City's credit or make it a guarantor of payment or surety for any contract, debt, obligation, judgment, lien, or any form of indebtedness. The Contractor further warrants and represents that it has no obligation or indebtedness that would impair its ability to fulfill the terms of this Agreement.

6. **INDEPENDENT CONTRACTOR RELATIONSHIP**. The Contractor is an independent Contractor and shall be treated as such for all purposes. Nothing contained in this Agreement or any action of the parties shall be construed to constitute or to render the Contractor an employee, partner, agent, shareholder, officer or in any other capacity other than as an independent Contractor other than those obligations which have been or shall have been undertaken by the City. Contractor shall be responsible for any and all of its own expenses in performing its duties as contemplated under this Agreement. The City shall not be responsible for any expense incurred by the Contractor. The City shall have no duty to withhold any Federal income taxes or pay Social Security services and that such obligations shall be that of the Contractor, other than those set forth in this Agreement. Contractor shall furnish its own transportation, office and other supplies as it determines necessary in carrying out its duties under this Agreement.

7. **INSURANCE.** Contractor shall, at its sole cost and expense, during the period of any work being performed under this Agreement, procure and maintain the minimum insurance coverages provided in Exhibit B to the ITN, in order to protect the City and Contractor against all loss, claims, damage and liabilities caused by Contractor, its agents or employees. **ANY EXCEPTIONS TO THE INSURANCE REQUIREMENTS IN THIS SECTION MUST BE APPROVED IN WRITING BY THE CITY**.

8. **TERMINATION AND REMEDIES FOR BREACH.**

A. If, through any cause within reasonable control, the Contractor shall fail to fulfill in a timely manner or otherwise violate any of its covenants, agreements or stipulations under this Agreement, the City shall have the right to terminate the Services then remaining to be performed. Prior to the exercise of its option to terminate for cause, the City shall notify the Contractor of its violation of the particular terms of the Agreement and grant Contractor thirty (30) days to cure such default. If the default remains uncured after thirty (30) days the City may terminate this Agreement, and the City shall receive a refund from the Contractor in an amount equal to the actual cost of a third party to cure such failure. If Contractor fails, refuses or is unable to perform any term of this Agreement, City shall pay for services rendered as of the date of termination.

(i.) In the event of termination, all finished and unfinished documents, data and other work product prepared by Contractor shall be delivered to the City and the City shall compensate the Contractor for all Services satisfactorily performed prior to the date of termination.

(ii.) Notwithstanding the foregoing, the Contractor shall not be relieved of liability to the City for damages sustained by it by virtue of a breach of the Agreement by Contractor and the City may reasonably withhold payment to Contractor for the purposes of set-off until such time as the exact amount of damages due the City from the Contractor is determined.

B. Termination for Convenience of City. The City may, for its convenience and without cause terminate the Services then remaining to be performed at any time by giving Contractor thirty (30) days written notice. The terms of Paragraph 8A(i) and 8A(ii) above shall be applicable hereunder.

C. Termination for Insolvency. The City also reserves the right to terminate the remaining Services to be performed in the event the Contractor is placed either in voluntary or involuntary bankruptcy or makes any assignment for the benefit of creditors.

9. **CONFIDENTIAL INFORMATION.** The Contractor shall not, either during the term of this Agreement or any time for a period of ten (10) years subsequent to the date of expiration of termination of this Agreement, disclose to any person or entity, other than in the discharge of the duties of the Contractor under this Agreement, any information which the City designates in writing as "confidential" (“Confidential Information”). The Contractor shall use Confidential Information solely for the purpose of performing its obligations under this Agreement and shall not use it for any other purpose, including for its own benefit or the benefit of any third party. The Contractor shall protect Confidential Information with the same degree of care it uses to protect its own confidential and proprietary information of like importance, but in no event with less than reasonable care. Upon expiration or termination of this Agreement, or at any time at the City’s request, the Contractor shall promptly return to the City or, if instructed by the City, destroy all documents and materials containing Confidential Information, including all copies thereof. As a violation by the Contractor of the provisions of this Section could cause irreparable injury to the City and there is no adequate remedy at law for such violation, the City shall have the right, in addition to any other remedies available to it at law or in equity, to enjoin the Contractor from violating such provisions. The Contractor shall in all respects comply with the Florida Public Records Act both as to the availability to the public of non-Confidential Information and as to the protection of exempt or confidential and exempt information when protection is mandated by applicable law. For security purposes, some of the information pertaining to the subject matter of this contract are protected by law from public disclosure.

10. **JURISDICTION, VENUE AND WAIVER OF JURY TRIAL.** This Agreement shall be interpreted and construed in accordance with and governed by the laws of the State of Florida. All parties agree and accept that jurisdiction of any dispute or controversy arising out of this Agreement, and any action involving the enforcement or interpretation of any rights hereunder shall be brought exclusively in the Eleventh Judicial Circuit in and for Miami Dade County, Florida, and venue for litigation arising out of this Agreement shall be exclusively in such state courts, forsaking any other jurisdiction which either party may claim by virtue of its residency or other jurisdictional device. In the event it becomes necessary for the City to file a lawsuit to enforce any term or provision under this Agreement and the City is the prevailing party then the City shall be entitled to its costs and attorney’s fees at the pretrial, trial and appellate levels. BY ENTERING INTO THIS AGREEMENT, CONTRACTOR AND CITY HEREBY EXPRESSLY WAIVE ANY RIGHTS EITHER PARTY MAY HAVE TO A TRIAL BY JURY OF ANY CIVIL LITIGATION RELATED TO THIS AGREEMENT. Nothing in this Agreement is intended to serve as a waiver of sovereign immunity, or of any other immunity, defense, or privilege enjoyed by the City pursuant to Section 768.28, Florida Statutes.

11. **NOTICES.** All notices and other communications required or permitted to be given under this Agreement by either party to the other shall be in writing and shall be sent (except as otherwise provided herein) (i) by certified or registered mail, first class postage prepaid, return receipt requested, (ii) by guaranteed overnight delivery by a nationally recognized courier service, or (iii) by e-mail with confirmation receipt (with a copy simultaneously sent by certified or registered mail, first class postage prepaid, return receipt requested or by overnight delivery by traditionally recognized courier service), addressed to such party as follows:

If to City:
City Manager
City of Doral, Florida
8401 NW 53rd Terrace
Doral, Florida 33166
rey.valdes@cityofdoral.com

With a copy to:
City Attorney
City of Doral, Florida
8401 NW 53rd Terrace
Doral, Florida 33166
lorenzo.cobiella@cityofdoral.com

If to Contractor:
Silka González
Enterprise Risk
Management
800 South Douglas Rd, 940 N
Coral Gables, FL 33134
sgonzalez@ermprotect.com

William G. McCullough
Shutts & Bowen
200 South Biscayne S 4100
Miami, FL 33131
wgm@shutts.com

12. **PUBLIC RECORDS.** The Contractor shall be required to comply with the following requirements under Florida's Public Records Law:

i. Contractor shall keep and maintain public records required by the City to perform the Services.

ii. Upon request from the City, Contractor shall provide the City with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided by Chapter 119, Florida Statutes, or as otherwise provided by law.

iii. Contractor shall ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the Contractor does not transfer the records to the City.

iv. Contractor shall, upon completion of the contract, transfer, at no cost to the City all public records in possession of the Contractor or keep and maintain public records required by the City to perform the Services. If the Contractor transfers all public records to the City upon completion of the contract, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided by Contractor to the City, upon request from the

City, in a format that is compatible with the information technology systems of the City.

IF CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CITY'S CUSTODIAN OF PUBLIC RECORDS AT 305-593-6730, CITYCLERK@CITYOFDORAL.COM, 8401 NW 53RD TERRACE, DORAL, FLORIDA 33166.

13. **AUDIT.** The Contractor shall make available to the City or its representative all required financial records associated with this Agreement for a period of three (3) years.

14. **NON-DISCRIMINATION.** The Contractor agrees to comply with all local and state civil rights ordinances and with Title VI of the Civil Rights Act of 1984 as amended, Title VIII of the Civil Rights Act of 1968 as amended, Title 1 of the Housing and Community Development Act of 1974 as amended, Section 504 of the Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990, the Age Discrimination Act of 1975, Executive Order 11063, and with Executive Order 11248 as amended by Executive Orders 11375 and 12086. The Contractor will not discriminate against any employee or applicant for employment because of race, color, creed, religion, ancestry, national origin, sex, disability or other handicap, age, marital/familial status, or status with regard to public assistance.

The Contractor will take affirmative action to ensure that all employment practices are free from such discrimination. Such employment practices include but are not limited to the following: hiring, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff, termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the City setting forth the provisions of this non-discrimination clause. The Contractor agrees to comply with any Federal regulations issued pursuant to compliance with Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. 708), which prohibits discrimination against the handicapped in any Federally assisted program.

15. **CONFLICT OF INTEREST.** The Contractor agrees to adhere to and be governed by the Miami-Dade County Conflict of Interest Ordinance Section 2-11.1, as amended; and by the City of Doral Code of Ordinances, which are incorporated by reference herein as if fully set forth herein, in connection with the Agreement conditions hereunder. The Contractor covenants that it presently has no interest and shall not acquire any interest, directly or indirectly which should conflict in any manner or degree with the performance of Services under this Agreement. The Contractor further covenants that in the performance of this Agreement, no person having any such interest shall knowingly be employed by the Contractor.

16. **INDEMNIFICATION AND WAIVER OF LIABILITY.** To the fullest extent permitted by law, the Contractor agrees to indemnify and hold-harmless the City, its agents, representatives, officers, directors, officials and employees from any claims, liabilities, damages, losses and costs, including, but not limited to, reasonable attorney fees to the extent cause, in whole or in part, by the negligence, error or omission of the Contractor or persons employed or utilized by the Contractor in performance of Services under this Agreement.

Contractor shall at all times hereafter indemnify, hold harmless and, at the City's option, defend or pay for an attorney selected by the City to defend City, its agents, representatives, officers, directors, officials and employees from and against any and all causes of action, demands, claims, losses, liabilities and expenditures of any kind, including attorney fees, court costs, and expenses, caused or alleged to be caused by the intentional or negligent act of, or omission of Contractor, including those of their employees, agents, servants, or officers, or accruing, resulting from, or directly related to the subject matter of this Agreement including, without limitation, any and all claims, losses, liabilities, expenditures, demands or causes of action of any nature whatsoever resulting from injuries or damages sustained by any person or property. In the event any lawsuit or other proceeding is brought against City by reason of any such claim, cause of action or demand, Contractor shall, upon written notice from City, resist and defend such lawsuit or proceeding by counsel satisfactory to City.

The provisions and obligations of this section shall survive the expiration or earlier termination of this Agreement. To the extent considered necessary by City, any sum due Contractor under this Agreement may be retained by City until all of City's claims for indemnification pursuant to this Agreement have been settled or otherwise resolved; and any amount withheld shall not be subject to payment of interest by City. The parties agree that One Hundred Dollars ($100.00) represents specific consideration to the Contractor for the indemnification set forth in this Agreement.

17. **COMPLIANCE WITH LAW.** Contractor shall comply with all laws, regulations and ordinances of any federal, state, or local governmental authority having jurisdiction with respect to this Agreement ("Applicable Laws") and shall obtain and maintain any and all material permits, licenses, approvals and consents necessary for the lawful conduct of the activities contemplated under this Agreement.

18. **CONFLICTING PROVISIONS.** The terms and conditions in this Agreement shall supersede and take priority over any inconsistent or conflicting provisions that are contained in any other document, including but not limited to Exhibit "A", and "B".

19. **PROHIBITION AGAINST CONTRACTING WITH SCRUTINIZED COMPANIES.** Pursuant to Florida Statutes Section 287.135, contracting with any entity that is listed on the Scrutinized Companies that Boycott Israel List or that is engaged in the boycott of Israel is prohibited. Contractors must certify that the company is not participating in a boycott of Israel. Any contract for goods or services of One Million Dollars ($1,000,000.00) or more shall be terminated at the City's option if it is discovered that the entity submitted false documents of certification, is listed on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List or has been engaged in business operations in Cuba or Syria after July 1, 2018. Any contract entered into or renewed after July 1, 2018 shall be terminated at the City's option if the company is listed on the Scrutinized Companies that Boycott Israel List or engaged in the boycott of Israel.

Contractor hereby certifies, pursuant to Section 287.135, Florida Statutes, that it is not on the Scrutinized Companies that Boycott Israel List created pursuant to Section 215.4725, Florida Statutes and that it is not engaged in a boycott of Israel.

In the event the Contract is for one million dollars or more, Contractor certifies that it is not on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List created pursuant to Section 215.473, Florida Statutes; and Contractor further certifies that it is not engaged in business operations in Syria. Submitting a false certification shall be deemed a material breach of contract.

The City shall provide notice, in writing, to the Contractor of the City's determination concerning the false certification. The Contractor shall have ninety (90) days following receipt of the notice to respond in writing and demonstrate that the determination was made in error. If the Contractor does not demonstrate that the City's determination of false certification was made in error, then the City shall have the right to terminate the contract and seek civil remedies pursuant to Florida Statute Section 287.135.

20. **E-VERIFY.** Florida Statute 448.095 directs all public employers, including municipal governments, to verify the employment eligibility of all new public employees through the U.S. Department of Homeland Security's E-Verify System, and further provides that a public employer may not enter into a contract unless each party to the contract registers with and uses the E-Verify system. Florida Statute 448.095 further provides that if a Contractor enters into a contract with a subcontractor, the subcontractor must provide the Contractor with an affidavit stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien. In accordance with Florida Statute 448.095, Contractor is required to verify employee eligibility using the E-Verify system for all existing and new employees hired by Contractor during the contract term. Further, Contractor must also require and maintain the statutorily required affidavit of its subcontractors. It is the responsibility of Contractor to ensure compliance with E-Verify requirements (as applicable). To enroll in E-Verify, employers should visit the E-Verify website (https://www.e-verify.gov/employers/enrolling-in-e-verify) and follow the instructions. The Contractor must retain the I-9 Forms for inspection, and update the E-Verify Affidavit, as may be needed. The Contractor's current E-verify Affidavit is included on page 31 of Contractor's ITN proposal, attached hereto as Exhibit "A".

21. **MISCELLANEOUS.**

A. In the event any provision of this Agreement is found to be void and unenforceable by a court of competent jurisdiction, the remaining provisions of this Agreement shall nevertheless be binding upon the parties with the same effect as though the void or unenforceable provisions had been severed and deleted.

B. This Agreement may be executed in multiple identical counterparts, each of which shall be deemed an original for all purposes.

C. This Agreement shall constitute the entire agreement between the parties with respect to the subject matter hereof, and it shall supersede all previous and contemporaneous oral and written negotiations, commitments, agreements and understandings relating hereto.

D. Any modification of this Agreement shall be effective only if in writing and signed by the parties to this Agreement.

E. No waiver of any provision of this Agreement shall be valid or enforceable unless such waiver is in writing and signed by the party granting such waiver.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement in duplicate on the day and year first written above.

WITNESS:

Signature

Casandra Yazdanpanah

Print Name

ENTERPRISE RISK MANAGEMENT, INC.

Silka Gonzalez

Silka M. Gonzalez, President

ATTEST:

BY: _

Connie Diaz
City Clerk

CITY OF DORAL

BY: Rey Valdes

Rey Valdes, City Manager

APPROVED AS TO FORM AND LEGAL SUFFICIENCY FOR CITY OF DORAL ONLY

BY: Lorenzo Cobiella

GASTESI, LOPEZ & MESTRE, PLLC,
City Attorney
By: Lorenzo Cobiella, Esq.

EXHIBIT "A"

ERM Proposal for ITN 2024-05

Inserted on Following Page

ERMProtect
Cybersecurity Solutions

Enterprise Risk Management, Inc. dba ERMProtect™

Response to Invitation to Negotiate

April 2, 2024

City of Doral

Invitation to Negotiate

ITN No. 2024-05

Independent IT Audit Services

Table of Contents

ERMProtect
Cybersecurity Solutions

March 27, 2024

Procurement Department
City of Doral
Florida

Dear Sir or Madam,

Enterprise Risk Management, Inc. dba ERMProtect, appreciates the opportunity to introduce our company and present this proposal to the City of Doral in response to its Invitation to Negotiate, ITN 2024-05 for Independent Audit Services.

Our company has a long trajectory and proven experience in all three areas sought by the city, including conducting IT security audits, digital forensics and penetration testing of all types, among other services. Since our funding 26 years ago, we have provided many of these exact cybersecurity services for various cities and agencies in South Florida and throughout the United States, keeping them safe from evolving cybersecurity threats. We have built a strong client service model that can be executed in a cost-effective manner to achieve high quality results while achieving important efficiencies.

Our consulting team is made up of highly qualified professionals at the forefront of the cybersecurity domain and are continuously up to date on the latest and emerging innovative technologies. As per our company requirements, they have advanced academic degrees in information security and hold information security and technical IT certifications including CISSP, C|EH, PCI/QSA, CISM, CISA, CRISC, and CITP. Our team includes astute compliance and risk management experts, highly skilled penetration testers and veteran forensic investigators, with a capacity to understand, anticipate and meet your most important needs. Also of note, we are one of only about 20 firms in the world certified to conduct forensic investigations of payment card breaches by the major credit card brands, a testament to our expertise in digital forensics.

Our project management methodology is a time-tested one that incorporates compliance with all the requirements our clients have and that emphasizes timely performance, precise issue mitigation, robust communication, and continuous quality control. We are constantly improving our technical methodologies to incorporate new standards and best practices.

I am confident ERMProtect is uniquely qualified to provide the City of Doral with the services it is seeking with the highest quality, dedication, and personalized attention of a trusted partner.

I confirm that I have the authority to make representations and agree to all the conditions stated on the solicitation. Thank you for considering our proposal.

Sincerely,

Silka M. Gonzalez
President & Founder - CISSP, CISA, CISM, CRISC, PCI QSA, CPA
Enterprise Risk Management, Inc. dba ERMProtect

Qualifications Statement

Enterprise Risk Management, Inc. dba ERMProtect is a Florida corporation founded in 1998 in response to the growing need for quality IT and Cybersecurity services. Our unwavering vision and values have shaped ERMProtect into an undisputed leader in cybersecurity.

With over 26 years of experience and outstanding credentials, ERMProtect is fully equipped to conduct an analysis of the IT security and access of the City of Doral.

Our company's ***extensive knowledge and experience*** in information security assessments, information technology (IT) risk management, penetration testing, security, auditing, telecommunications, information systems, computer forensics, incident response, investigations, and regulatory compliance, equips us with the background, competence and qualifications required to provide the City of Doral with the security services it seeks.

We are a ***trusted, go-to provider*** of comprehensive information security services to more than 450 clients in 39 industry verticals in the United States, Latin America, the Caribbean and Europe***.*** ***Government clients at the County, City and Local level make up one of the most important groups we serve***.

We are a minority, women-owned small firm that has adapted, evolved, and excelled because it emphasizes education, training, integrity, adaptability, service, and diversity of people and ideas. ERMProtect's highly trained and experienced professionals are devoted to protecting your networks, information systems and data while promising a superior level of quality and professionalism. E***RMProtect's team has the appropriate expertise, education, and certifications.***

Besides our experience and qualifications, our uniqueness stands out for the following reasons:

- ✓ ERMProtect operates with a focus on the ***firm's key values: ethics, trust, excellence, service, can-do attitude, passion.***
- ✓ ERMProtect provides ***customized and cost-effective solutions.***
- ✓ ERMProtect provides unparalleled dedication to clients and unmatched customer service. We are ***always available*** to answer questions, without passing the cost to you.
- ✓ ERMProtect believes in ***knowledge transfer***. We never leave the job until your staff has the know-how to achieve RFP objectives.

Since our founding, ERMProtect has provided clients with a full complement of cybersecurity services and products that identify, manage, and minimize data security risk. ERMProtect provides services in four (4) major areas:

1. **Cybersecurity Assessments and IT Audits**

   Through its years in service, ERMProtect has performed thousands of security assessments and IT control reviews of various types to help clients identify vulnerabilities and build up their defenses. This area has always been one of our leading sources of revenue.

   The most common are:

   - All types of Penetration Testing (external, internal, web/mobile applications, wireless, segmentation tests and others required by the Payment Card Industry (PCI) Council,

Cloud Infrastructure, ICS/SCADA, Physical Site, IoT, Social Engineering and Regulatory Compliance).
- Assessments required by the Payment Card Industry (PCI) Council – PCI QSA, PCI Scans, PCI Penetration Tests
- General Risk Assessments oriented towards the compliance of different federal, state or local laws (HIPAA, FISMA, FERPA, GDPR, GLBA, FACTA, FedRamp), for the Information Technology Area, or the entire organization.
- Different types of Cybersecurity Assessments with different scopes, requirements and use of various security standards such as NIST, ISO27001 and CIS security model.
- SOC 2 Attestations and Comprehensive security and IT Audits with varying scopes.

2. Co-Sourcing of Cybersecurity Services

We have provided consulting, guidance, implementation, and remediation services to many clients, both fully and partially depending on their needs. Some examples of these include:

- Review/Implementation of security plan, standards, policies, procedures
- CISO co-sourcing or full outsourcing.
- Incident Response on-demand
- Implementation/remediation of security for specific areas and technologies
- On-demand security advisory services
- Performance of third-party vendor security assessments

3. Digital Forensics

Digital Forensics is one of ERMProtect's fastest growing areas of business. Our digital forensic and incident response experts help organizations stop, recover from, and get to the bottom of a breach with a thorough forensic investigation. This area includes:

- Investigation of Security Incidents and Data Breaches of all types
- Investigation of security breaches related to the Payment Card Industry (PCI PFI)
- Fraud or internal misconduct investigations
- Litigation Support
- Crypto Investigations

4. Security Awareness Training and Social Engineering

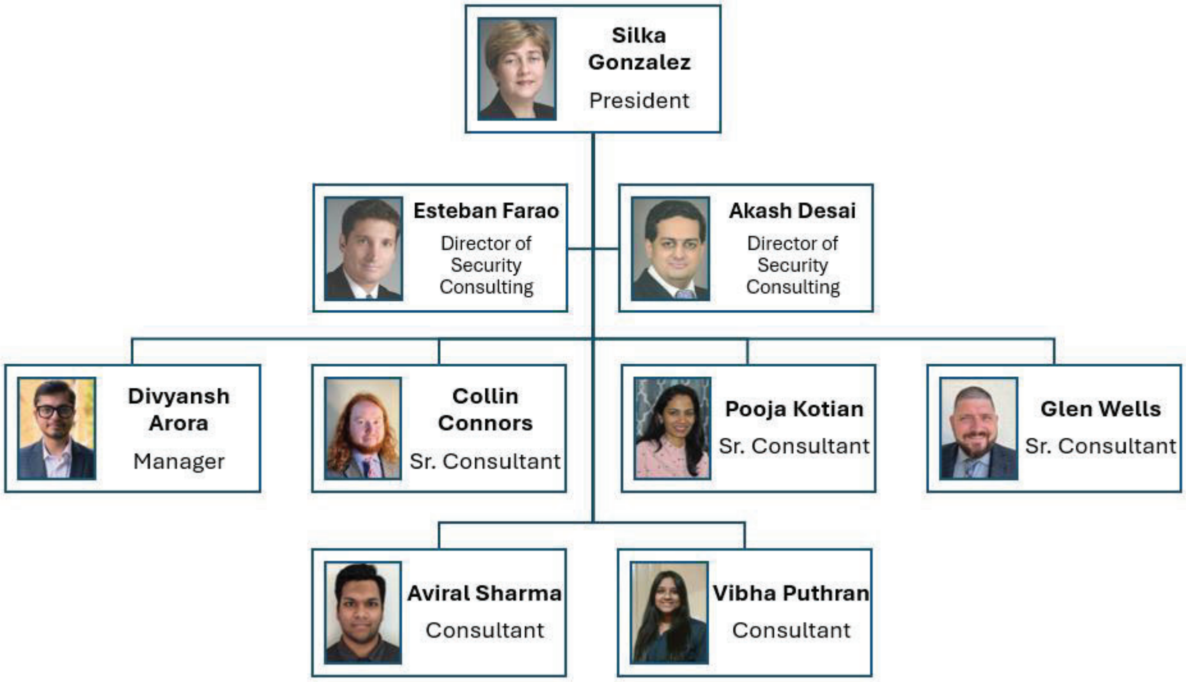
ERMProtect has developed various types of security awareness training content which can be delivered in any of the following ways:

- Through an LMS System, by subscription – many courses covering many security areas.
- "A la Carte" – clients can choose courses in SCORM version to download into their own LMS system.
- Customized security training, tailored to the needs of the client – technical and non-technical.

ERMProtect also developed its own tool for performing phishing, vishing and smishing tests. These tests are customized and automated for the needs of each client.

A. Organizational Chart

Below you will find ERMProtect's project team organizational chart, including names and functions. This is our consulting team, which is able to provide our clients with a high level of expertise with a very personalized approach. We are available to attend to our clients at a very short notice, they know they can always count on us to understand and anticipate their needs.



ERMProtect works is a Prime proposer; we perform all our projects with our own staff, we do not use subcontractors.

In the Project Team's Experience section, we provide a short biography of each of our consultants, and we also provide their resumes in the Appendix: ERMProtect Team Resumes.

B. Proposer's Experience

The following are references and descriptions of recent work ERMProtect has performed for various clients, many of them government entities. These projects include various of the Cybersecurity Services we provide and attest to our experience. Please find also Exhibit A – Proposer Qualification Statement, as an attachment to this proposal.

- **Miami-Dade County**
  ERMProtect has provided various cybersecurity services to the Miami-Dade County, the 7th largest county in the United States, with an annual operating budget of more than $9 billion. We completed a five-year contract to provide all types of penetration testing (external, internal, wireless, web application, segmentation), PCI QSA services, digital forensic services, and Security Risk Assessment done based on the SP 800-30 r1 "Guide for Conducting Risk Assessments" and using the NIST Cybersecurity Framework (CSF) 1.1 as a control baseline. The engagement

includes testing of 500 internal IP addresses, 210 external IP addresses and 28 applications used by executive, administrative, operational, transportation service departments and airports. This contract was extended for an additional year (2024) and ERMProtect was just awarded the next 6-year contract to provide these same and additional services starting in 2025. Both contracts include a clause to request any type of cybersecurity service at predetermined negotiated prices.

Individuals who have worked on these projects: Esteban Farao, Akash Desai, Divyansh Arora, Collin Connors, Aviral Sharma, Pooja Kootian and Vibha Puthran.

Contact:	**Lars Schmekel -** lars.schmekel@miamidade.gov
Contact Title:	Chief Security Officer
Telephone:	305 596-8779

- <u>**City of West Palm Beach**</u>
  ERMProtect has been servicing the City of West Palm Beach for more than 6 years. All of our cybersecurity consultants have participated in performing various cybersecurity projects such as:

  - ✓ *Comprehensive Cybersecurity Assessment*s of the City and Police departments in order to identify security deficiencies in the logical, physical and administrative security controls used. Based on the results, ERMProtect prepared action plans to remediate, setting up priorities based on the level of the security risk, and provided guidance to the IT personnel to implement the necessary security measures.

  - ✓ Different types *of Vulnerability Assessments and Penetration Testing* including external, internal and wireless networks, as well as web applications. Upon completion, ERMProtect consultants discussed with the IT personnel of the city the findings noted during the various assessments and guided them in implementing the necessary security controls. We then performed re-testing to ensure the noted issues were properly corrected.

  - ✓ A *Comprehensive Assessment of PII information* throughout all the infrastructure and systems of the entire city using an automated software. Performed an evaluation of the assignment of PII, identified all the weaknesses and performed corrections to ensure this private information was only assigned to limited authorized users.

  - ✓ A *Comprehensive Analysis of the Windows Active Directory*. ERMProtect consultants reviewed groups, structure and users of the entire city, identified deficiencies and security issues and assisted the city in implementing the necessary changes to improve the group structure and access assignments.

  - ✓ Technical Security Audits of predetermined scope.

  - ✓ Assistance in the development of security plans, policies and procedures.

  - ✓ On-going cybersecurity consultation and guidance, assistance with any type of security assignment requested.

Individuals who have worked on these projects: Esteban Farao, Akash Desai, Divyansh Arora, Collin Connors, Aviral Sharma, and Vibha Puthran.

Contact:	**Paul Jones -** pjones@wpb.org
Contact Title:	Chief Information Officer
Telephone:	561 578-2420/561 822-1258

- **City of Coral Gables:**
  ERMProtect has been in business with the City of Coral Gables for more than six years. The scope of work performed includes yearly PCI DSS audits, external, internal, web application and segmentation penetration testing, Access to Qualys portal for ASV scans and additional consulting services such as security training and phishing tests. Regarding training, ERMProtect conducted tailored security awareness training sessions for various employee groups, including IT professionals, general staff, and executives, aligning the content with their specific job roles. We have also provided digital forensic services to the City of Coral Gables.

Contact:	**Nelson Gonzalez -** ngonzalez@coralgables.com
Contact Title:	Assistant Information Technology Director
Telephone:	305 460-5076

Individuals who have worked on these projects: Esteban Farao, Akash Desai, Divyansh Arora, Collin Connors, Aviral Sharma, and Pooja Kotian.

- **Miami Dade School Board**
  We performed a Cybersecurity Risk Assessment based on NIST Standard SP 800-30 r1 guidance for conducting Risk Assessment using NIST Cybersecurity Framework CSF 1.1 as control baseline. Performed various penetration tests including external-internal-wireless networks, web and mobile applications and phishing tests. We are currently performing Denial-of-Service penetration tests.

Contact:	**Luis Baluja** – luisbaluja@dadeschools.net
Contact Title:	District Director, Information Technology Audits
Telephone:	305-995-1318

Individuals who have worked on this project: Esteban Farao, Akash Desai, Divyansh Arora, Pooja Kotian, Collin Connors, Aviral Sharma, Vibha Puthran and Glen Wells.

- **Broward County**
  In the last two years we have performed several projects for the Broward County including an IT Risk Assessment done based on the SP 800-30 r1 "Guide for Conducting Risk Assessments" and using the NIST Cybersecurity Framework (CSF) 1.1 as a control baseline, a PCI Security Assessment for the Aviation Department.
  We performed an IT Audit and Penetration testing and a SCADA Security Review for the Water and Waste Department. We also performed a Risk assessment Gap Analysis against NIST Standard SP 800-82 r3 operational technology (OT) security as the baseline. We also worked on a project to review the Broward County Incident Response Plan and suggest recommendations

to improve their existing plans.

Broward Waste and Wastewater Services

Contact Name:	Alan Garcia, agarcia@broward.org
Contact Title:	Director
Telephone:	(954) 831-0702

Broward County - ETS

Contact Name:	Gail McGowan, gmcgowan@broward.org
Contact Title:	ETS, IT Business Services, Security & Compliance
Telephone:	(954) 357-6147

Broward County – Aviation Department

Contact Name:	Karen Macdougall – kmacdougal@broward.org
Contact Title:	Information Technology Specialist
Telephone:	954 359-7213

Individuals who have worked on these projects: Esteban Farao, Akash Desai, Divyansh Arora, Collin Connors, Aviral Sharma and Pooja Kotian.

- **City of Saint Petersburg**
  ERMProtect has been in business with the City of Saint Petersburg since 2021. The services provided include PCI DSS audits, comprehensive cyber security assessments using the CIS Framework as baseline of security controls, penetration testing services (internal, external, phishing, wireless) and an incident response tabletop top exercise. ERMProtect played a crucial role in assisting the city by outlining the scope of the environment and collaborating with the acquirer to confirm the specific types of controls to be included in the PCI/QSA/ROC. Additionally, ERMProtect provided ongoing support throughout the remediation process while upholding its independence.

Contact:	**Brian Campbell** – brian.campbell@stpete.org
Contact Title:	Information Technology Security Officer
Telephone:	727 892-5503

Individuals who have worked on these projects: Esteban Farao, Akash Desai, Divyansh Arora, Pooja Kotian, Collin Connors, Aviral Sharma and Glen Wells.

C. Project Team's Experience

ERMProtect's team has highly respected educational and professional qualifications. Our professionals have earned master's degrees, specifically in information security and networking, from esteemed institutions of learning such as the Carnegie Mellon University, Purdue University, John Hopkins, MIT, Georgia Tech and the University of Miami, and hold reputed professional information security certifications such as the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), PCI Approved Qualified Security Assessor (QSA), PCI Professional Forensic Investigator (PFI) and the Certified Information Systems Auditor (CISA), to name only a few.

The following is a summary of our team biographies. Their resumes are also provided in the **Appendix: ERMProtect's Team resumes.**

Silka Gonzalez

President and Founder of ERMProtect. Silka has more than 35 years of experience in the field of cybersecurity. Since 1998, ERMProtect has provided cybersecurity, computer forensics and technical compliance services to more than 450 recurring clients in 39 different industries worldwide. Prior to founding ERMProtect, she was a manager of IT and business services at Price Waterhouse. She also served as Manager of Information Systems Auditing for Diageo PLC and Manager of Information Systems Security for American Bankers Insurance Group (now Assurant Solutions).

Silka received Bachelor's degrees in both Computer Information Systems and Accounting from Xavier University in Cincinnati, Ohio and she received a Master's degree in Accounting Information Systems from Florida International University in Miami. Silka also completed and Entrepreneurial Master's Program at the Massachusetts Institute of Technology (MIT) in Boston. Silka's **certifications include CISSP, CISM, CISA, CITP, CRISC, PCI-QSA, CPA and ISO27001 Auditor.**

Silka is a published author, addressing current issues in cybersecurity, IT auditing, regulatory compliance and computer forensics. Silka is frequently sought out by local and national newspapers and magazines as a subject matter expert in cyber security. She also appears in local and national news as a cybersecurity expert.

Silka previously served as a board member of the Florida International Bankers Association (FIBA), as member of Xavier University's President Council, as president of the Miami chapter of the Institute of Internal Auditors, and the boards of ISACA South Florida (Information Systems Audit and Control Association) and ALPFA (Association of Latino Professionals in Finance and Accounting). She has also served on Florida's judicial nomination commission for workman's compensation judges.

Esteban Farao

Director of Information Security Consulting Services. Esteban has worked at ERMProtect for 21 years and has more than 29 years in the Cybersecurity industry. As a cybersecurity expert, he has extensive experience in all types of ethical hacking, performance of IT and\or cybersecurity audits, performance of security implementations, performance of all types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO27001 standards, state and federal cybersecurity laws and regulations, and cybersecurity frameworks. Esteban has also been involved in many large PCI Cybersecurity audits, compliance, and remediation projects for all the largest and most complex clients of ERMProtect. He also has extensive experience in digital forensics project investigating regular security breaches, credit card breaches, fraud investigations, internal misconduct, and litigation support cases. Additionally, Esteban has developed, enhanced, and tested many business continuity plans and security incident response plans as well as security strategies, plans, policies and procedures. He also has developed and delivered different types of cybersecurity trainings, (including complex security incident response table talk training to an entire City), assist many large clients with on-going consultation, publish cybersecurity articles and is frequently interviewed by television networks to share his security expertise.

Prior to joining ERMProtect, Esteban worked 6 years for PwC Argentina where we performed different types of cyber security projects. He also participated in global attack and penetration testing assignments for PwC in London. Esteban hold a Bachelor's Degree in Computer Science, a Master degree in Computer Information Systems, and a Master in Business Administration (MBA). He holds the following IT **Security Certifications: CISSP, CISA, CRISC, C|CISO, CEH, PCIP, PCI QSA, PCI PFI and EnCe, CNDA, CDPSE, and ISO27001 Auditor.**

Akash Desai

Director of Information Security Consulting Services. Akash has worked at ERMProtect for 17 years. As a cybersecurity expert, he has extensive experience in all types of ethical hacking, performance of IT and\or cybersecurity audits, performance of security implementations, performance of all types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO27001 standards, state and federal laws and regulations, and cybersecurity frameworks. Akash has also been involved in many large PCI Cybersecurity audits, compliance, and remediation projects for all the largest and most complex clients of ERMProtect. Akash has developed, enhanced, and tested many business continuity plans and security incident response plans as well as security strategies, plans, policies and procedures. He developed ERMProtect's security awareness training practice which offers off-the-shelf and customized training for employees using animations, games, mini lectures, etc. Akash as developed and delivered different types of cybersecurity trainings, assist many large clients with on-going consultation, publish cybersecurity articles and is frequently interviewed by magazines, newspapers, and television networks to share his security expertise.

Prior to working for ERMProtect, Akash worked for CERT for two years specializing in security incident response. Akash holds a Bachelor's degree in Computer Science and a Master degree in Information Networking with a Cybersecurity specialization from Carnegie Mellon University and the following IT **Security Certifications: CISSP, CISA, CEH, PCI QSA and PCIP**.

Pooja Kotian

Manager, Information Security Consulting Services. Pooja has worked at ERMProtect for 9 years, and has more than 12 years of experience as a Senior Systems Engineer and as an Information Security Consultant overseeing many types of cyber security projects. As a cybersecurity expert, she has extensive experience in all types of ethical hacking, performance of IT and\or cybersecurity audits, performance of security implementations, performance of all types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO27001 standards, state and federal laws and regulations, and cybersecurity frameworks. Pooja has also been involved in many large PCI Cybersecurity audits, compliance, and remediation projects for all the largest and most complex clients of ERMPROTECT. Pooja has developed, enhanced, and tested many business continuity plans, security incident response plans as well as security strategies, plans, policies and procedures.

She began her career as a Systems Engineer for Infosys before joining ERMProtect in 2015 where she was a mobile and web application developer with significant experience testing applications for issues and vulnerabilities so they can be corrected. She has a Bachelor's degree in Engineering, Information Technology. Pooja holds the following **security certifications**: **Infosys Quality Foundation, Dotnet Technology 101 and STAR Certification** (internal to Infosys).

Divyansh Arora

Manager, Information Security Consulting Services. With three years of experience at ERMProtect, Divyansh has been involved in a wide range of activities, including ethical hacking, IT and cybersecurity audits, security implementations, and various cybersecurity risk assessments using NIST cybersecurity standards, ISO27001 standards, and cybersecurity frameworks. He has also contributed to PCI Cybersecurity audits, compliance, and remediation projects for some of ERMProtect's largest clients. Additionally, Divyansh has participated in digital forensics projects, investigating security breaches, credit card breaches, fraud cases, internal misconduct, and litigation support.

Before earning his master's degree in Information Technology- Information Security from Carnegie Mellon University, Divyansh obtained a bachelor's degree in Computer and Communications. Prior to joining ERMProtect, he served as a Senior Cybersecurity Analyst at PricewaterhouseCoopers for nearly two years. During his time at PwC, Divyansh conducted numerous vulnerability assessments and penetration tests for web applications, networks, Android & iOS mobile applications, and IoT devices such as CCTV and C&C displays for both government and private clients. He also gained experience as an intern at McKinsey Investment Office, focusing on cloud security research.
Security certifications: OSCP, CMWAPT

Collin Connors

Senior Information Security Consultant. Collin has worked for 5 years at ERMProtect. He has extensive experience in performing all types of penetration and phishing testing, as well as, cybersecurity audits, various types of cybersecurity risk assessments using all types of NIST cybersecurity standards, ISO 27001 standards and cybersecurity frameworks. Additionally, he has provided services surrounding various federal and state cybersecurity laws (e.g. GLBA, FACTA, HIPAA). Collin also has extensive knowledge and experience in cryptocurrency investigations and has participated in several Digital Forensics projects. Some of these cryptocurrency investigations have also resulted in people's conviction to prison. He has developed various automated system products for ERMProtect including an automated phishing tool, a phishing email analysis tool, and an automated system that performs SOC2 Assessments.

Collin also oversees the company's internal IT and security. He has a lot of experience in conducting cybersecurity trainings for external clients as well as ERMProtect's internal staff. His on-going consultations and customized trainings are very highly regarded and impactful. He is frequently interviewed by television networks to share his research and knowledge regarding cryptocurrency, blockchains and cybersecurity.

Apart from working at ERMProtect, Collin is also a part-time teacher at the University of Miami where he teaches cybersecurity and computer programming to undergraduate students. He holds a bachelor's degree in computer science and mathematics and is expected to complete his PhD Degree in May 2025. His PhD research includes the use of artificial intelligence to detect malware and various novel implementations of blockchain technology. **Security certification: CISc.**

Aviral Sharma

Information Security Consultant. Aviral worked as a student intern for ERMProtect during the summer of 2022, and he became a full-time employee in February 2023. During his time at ERMProtect he has performed security risk assessments, data compliance assessments, IT audits and various types of penetration testing.

Aviral has a Bachelor's degree in Computer Science and Engineering with a specialization in Information Security, and received his master's degree in Information Technology – Information Security from the prestigious Carnegie Mellon University. At CMU he underwent advanced training in code reviews, digital forensics, and vulnerability assessments for mobile applications.

Vibha Puthran

Information Security Consultant. Vibha worked as a student intern for ERMProtect during the summer of 2023 and started her full-time job with us as an Information Security Consultant in February of this year.

She performs incident response cases and digital forensic investigations for the firm’s diverse client base. She specializes in incident response investigations like ransomware, tabletop exercises, incident planning and management and security awareness training. She has also participated in IT audits.

Prior to joining ERMProtect, she worked as a Cybersecurity Consultant for PwC in India for one and a half years. Vibha has a bachelor’s degree in Computer Science-Engineering, a postgraduate Diploma in Cyber Law and Cyber Forensics from the National Law School of India University, and a Master’s degree in Information Security from Carnegie Mellon University. Security Certifications: EC Council Incident Handler, Microsoft Azure Fundamentals, CyberArk Certified Trustee, Splunk 7. X Fundamentals Part 1, Autopsy and Cyber Triage DFIR, ICSI CNSS and AWS Cloud Practitioner.

Approach and Methodology

ERMProtect understands that City of Doral seeks to conduct a digital forensics analysis of its IT security systems, including a focus on folder permissions within the network file shares. As a result, City of Doral aims to conduct an analysis and evaluation of its IT security systems to provide transparency, accountability, and to enhance its security posture.

Based on ERMProtect’s understanding, the following reviews and tasks are required to achieve the City of Doral´s objectives:

- IT Security Policies and Procedures Review
- Audit of Existing Access Controls
- Change Management Process Review
- Comprehensive Digital Forensic Audit
- Any other cybersecurity service such as Penetration Testing or Vulnerability Assessment which may be needed to better evaluate the City’s security posture
- Protocol Recommendations for Enhanced Security

ERMProtect’s project approach along with the detailed technical methodologies for each of the project tasks above has been provided below. For Penetration Testing we are presenting below the methodology for Internal and External Network Penetration Testing, but we can provide others such as for wireless networks, web applications if requested.

A. Technical Approach

Methodologies

- **IT Security Policies and Procedures Review**

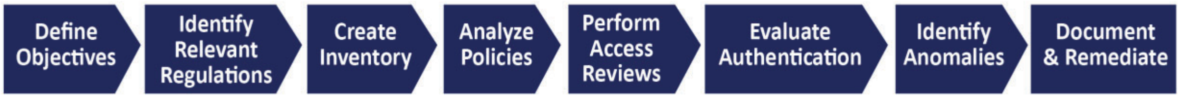
Reviewing IT security policies and procedures involves a comprehensive evaluation of documented guidelines, protocols, and practices to ensure they align with industry standards, regulatory requirements, and organizational objectives. ERMProtect begins with a thorough examination of existing policies, including access control, data protection, incident response, and compliance frameworks. This entails assessing the clarity, completeness, and relevance of policies to current security challenges and organizational needs. Next, procedures are scrutinized to determine their effectiveness in implementing policy directives, with a focus on user awareness, training, and enforcement mechanisms.

Following the initial review, a comparative analysis is conducted to benchmark existing policies against industry best practices, regulatory mandates, and emerging threats. This involves referencing authoritative sources such as NIST guidelines, ISO standards, and regulatory frameworks applicable to the organization's industry. Identified discrepancies or deficiencies are prioritized based on risk assessment criteria, considering the potential impact on confidentiality, integrity, and availability of critical assets. Recommendations for policy enhancements, updates, or new initiatives are formulated, emphasizing the importance of proactive risk management and continuous improvement. The final step involves documenting findings and proposed changes in a comprehensive report, highlighting areas for enhancement and outlining a roadmap for policy refinement and implementation. Continuous monitoring and periodic reviews are recommended to ensure ongoing compliance and alignment with evolving security requirements and organizational objectives.

- **Audit of Existing Access Controls**

Reviewing user access controls to a system involves a systematic approach to ensure security and compliance. ERMProtect's high-level methodology to audit existing access controls is depicted below:

ERMProtect Methodology: Audit of Existing Access Controls



Define Objectives and Scope - Clarify the purpose of the access control review. Define the scope of the review, including systems, users, and data to be assessed.

Identify Regulatory Requirements and Best Practices - Understand relevant regulations (e.g., GDPR, HIPAA) and industry best practices. Ensure that access controls align with these requirements.

Inventory User Accounts and Permissions - Compile a comprehensive list of user accounts and their associated permissions. Document the roles and responsibilities of each user.

Analyze Access Control Policies - Review the system's access control policies, including role-based access control (RBAC), attribute-based access control (ABAC), and discretionary access control (DAC). Assess whether access controls are properly configured and enforced.

Perform User Access Reviews - Using the information compiled in the preview's phases, verify that users have appropriate access levels based on their roles and responsibilities and identify and address any excessive permissions or unauthorized access.

Assess Authentication Mechanisms - Evaluate the effectiveness of authentication methods (e.g., passwords, multi-factor authentication). Ensure that strong authentication measures are in place, especially for privileged accounts.

Review Access Logs and Monitoring - Examine access logs and monitoring systems for suspicious activities. Identify any unauthorized access attempts or anomalies.

Document Findings and Remediate Issues - Document all findings from the access control review. Prioritize and address any identified issues or gaps in access controls.

- **Change Management Process Review**

Performing a change management assessment involves conducting a thorough examination of an organization's change processes to ensure they are efficient, effective, and compliant. ERMProtect's change management process review entails evaluating the organization's change control policies and procedures, including how changes are initiated, assessed for impact, prioritized, and authorized. Additionally, ERMProtect assesses the communication channels used to disseminate information about changes, the documentation practices for recording change details and outcomes, and the methods for monitoring and evaluating the success of implemented changes. By scrutinizing these aspects, organizations can identify any gaps, inefficiencies, or areas for improvement in their change management practices, enabling them to enhance agility, minimize risks, and optimize their ability to adapt to evolving business needs.

- **Comprehensive Digital Forensic Audit**

ERMProtect understands that City of Doral requires a very specific type of digital forensic audit that comprehensively covers the following:

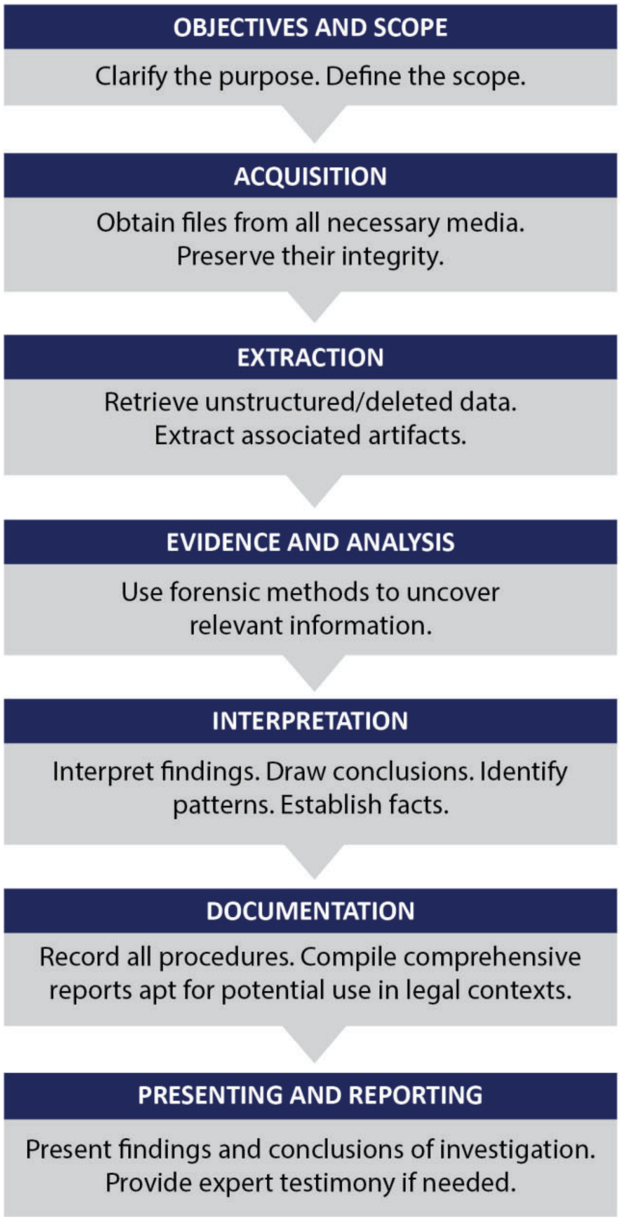
- ✓ Performing a digital forensic analysis of elected official file shares (approximately 30 top-level folders), including:
  - ○ Examination of all permissions set on such folders since 2018.
  - ○ Analysis of creation dates for all such folders within the file share.
  - ○ Documentation of all instances when permissions were changed or occasions when security-related actions were logged since 2018.
  - ○ Review of access logs for folders by users who were not the designated mayor, council member, or staff.
  - ○ If possible, identify whether documents or data accessed by unauthorized internal or external users were copied, moved, uploaded, or downloaded.

- ✓ Preparing a detailed timeline of all instances of access, including the specified user, from January 1, 2018, through the present date, including the first and last recorded accesses, and further addressing the following:
  - ○ Specify when folders were created and what permissions were initially granted.
  - ○ Identify all instances where changes were made in permissions for each folder within the file share, including identification of which changes in permissions were made.
  - ○ Indicate all instances where elected officials or their staff accessed folders belonging to other council members.
  - ○ Identify any instances of access by external (unauthorized) users.

- ✓ Identifying other areas of concern.

Conducting a forensic analysis of file systems is a meticulous endeavor demanding expertise at every juncture. Below are the steps to effectively analyze a file system for potential evidence crucial in a forensic investigation.

ERMProtect Methodology:
Comprehensive Digital Forensic Audit



OBJECTIVES AND SCOPE

Clarify the purpose. Define the scope.

ACQUISITION

Obtain files from all necessary media. Preserve their integrity.

EXTRACTION

Retrieve unstructured/deleted data. Extract associated artifacts.

EVIDENCE AND ANALYSIS

Use forensic methods to uncover relevant information.

INTERPRETATION

Interpret findings. Draw conclusions. Identify patterns. Establish facts.

DOCUMENTATION

Record all procedures. Compile comprehensive reports apt for potential use in legal contexts.

PRESENTING AND REPORTING

Present findings and conclusions of investigation. Provide expert testimony if needed.

Objectives and Scope - Clarify the purpose of the forensic investigation. Define the scope of the analysis, the devices, type of data, locations, etc.

Acquisition - The system must be safeguarded to guarantee the safety of all data and equipment.

Specifically, all media necessary for forensic analysis should be acquired and protected against unauthorized access. These files should be obtained from all storage media, including hard drives and portable devices. After acquisition, forensic investigators must create duplicates to preserve the integrity of the original files and prevent any potential alterations. During this phase ERMProtect will use tools and techniques to obtain a bit-by-bit copy of the original data, preserving its integrity.

Extraction - This phase involves the retrieving of unstructured or deleted data and needs to be processed for forensic investigation. This phase also encompasses the extraction of all associated artifacts essential for achieving the investigation's objectives, amplifying the depth and scope of the analysis.

Evidence Analysis - The type of analysis that needs to be performed is tied to the objectives and scopes. Examine the acquired data using forensic tools and techniques to uncover relevant information. Search for deleted files, hidden data, or any other artifacts pertinent to the investigation. Analyze file metadata, timestamps, and access logs to reconstruct events and timelines.

Interpretation - Interpret the findings from the analysis phase to draw conclusions and establish facts. Correlate the discovered evidence with the incident under investigation. Identify patterns, anomalies, or correlations that may provide insights into the incident.

Documentation - Record all procedures undertaken throughout the investigation, encompassing the tools employed, methodologies adhered to, and outcomes achieved. Compile comprehensive reports outlining the investigative journey, encompassing the evidence gathered and the deductions drawn. Guarantee that the documentation is precise, transparent, and apt for potential use in legal contexts.

Presentation and Reporting - Present the findings and conclusions of the investigation to stakeholders. Provide expert testimony if required in legal proceedings, explaining the methodology employed and the significance of the evidence. Ensure that the presentation and reporting are tailored to the audience, conveying complex technical information in an understandable manner.

- **External/Internal Network Vulnerability Assessment and Penetration Testing**

By conducting vulnerability assessments and penetration testing, ERMProtect will assess the overall network security including the network perimeter devices residing on network segments (DMZ and internal) and the Internet for potential vulnerabilities that could expose critical organizational systems and applications; customer information; organization information, and financial assets. This assessment will be conducted combining the tools and techniques used by malicious "hackers" with disciplined scientific procedures to provide unique insight into the state of security in the information systems environment of the organization. The security assessment will provide the organization with a diagnosis of network vulnerabilities from an external perspective (from the Internet into the organization’s internal network) and an internal perspective (from the internal network to the Internet). Networked devices including firewalls, routers, switches, servers, printers, remote-access devices, mainframes, middleware, and backend services connected to the Internet will all be assessed.

The engagement will provide the organization with an overall security assessment of the organization that addresses risk exposures noted during the evaluation. The results of this review will help strengthen the established security controls, standards, and procedures to prevent unauthorized access to the organizational systems, applications, and critical resources. As a result of our tests, we will prepare detailed work papers documenting the tests performed, and a report of our findings including recommendations for external access security controls.

ERMProtect penetration testing methodology was designed taking in considerations OWASP Testing Guide, PTES Technical guidelines, NIST 800-115, NIST 800-53, NIST-SP800-42, PCI DSS Guidance (March 2015/September 2017), OSSTMM, CWE/ SANS top 25, and experience from previous engagement.

In general terms, ERM penetration testing methodology is divided into 4 phases: Scenery definition, gathering information, intrusion, and report preparation. This methodology is applicable for any type of penetration test such as Application pentest, Wireless pentest, Bluesnarfing, network penetration test, red teaming, mobile pentest, ioT pentest, cloud pentest, and Social Engineering. The only thing that changes is the Scenery definition and the way the test are performed.

All our penetration testing assessments will follow the following rules of engagement unless there are specific requirements or definitions in Scenery Definition phase:

- No denial-of-service attacks will be used
- No un-trusted tools and techniques will be used
- No active backdoor or Trojans will be installed
- No sensitive data will be copied, modified or destroyed
- The specific tasks of the tests performed will be documented
- The operational impact to the networks will be maintained to the minimum

Important Notes

- Our review of the areas mentioned above assumes that internal personnel will help with the coordination efforts. The help required, though, will be minimal.
- ERMProtect shall use various proprietary and in-house tools and scripts for the purpose of this project.
- ERMProtect fully understands that organization require “near zero downtime”. In this light, all tests shall be planned and scheduled to be conducted in night or early morning time windows to minimize the risk of downtime.
- For internal testing, ERMProtect professionals will require the organization to help connect a virtual scanner appliance internally in a way that the appliance can obtain an internal IP address with access to the scope IPs and segments. The client will be expected to provide minor assistance in terms of guiding where such connection points are located. Additionally, in the case of remote testing, VPN access will need to be facilitated with access to the internal scope IPs and segments.

- **Protocol Recommendations for Enhanced Security**

As a result of the comprehensive digital forensic audit, ERMProtect will provide documented recommendations to City of Doral including changes to security access protocols and enhanced security to ensure compliance with such protocols.

Project Deliverables

- **KEY DELIVERABLE: ERMProtect's Reports**

For each of the phases of the project covered above, ERMProtect's project team will document all findings in a final report. This report will provide visibility into specific weaknesses and deficiencies in the security controls employed or inherited by the technical infrastructure and/or assessment area in scope. The report will make comprehensive recommendations on each finding along with precise instructions and action items on how findings can be best remediated.

Before finalizing a report, ERMProtect will meet with key client personnel to discuss a draft version of the report. System managers and key technical client staff will then have the opportunity to review and discuss information gathered, findings, and/or recommendations in order to avoid any misunderstanding in identified report items. ERMProtect will obtain and incorporate all draft report feedback to then document the final reports. All final reports will be provided to the client in both physical and electronic forms. The electronic form can be made available in a specific format the client wishes (e.g. spreadsheet of findings, editable document, etc.).

The final report shall be divided into various sections. Each section is described below:

Executive Summary

- **Executive Summary:** An executive-level summary free of jargon and buzz-words directed at senior management. It will cover the objective, scope, approach, overall assessment results, and risk/severity levels.
- **Summary of Findings and Recommendations:** ERMProtect will describe the environment and high-level findings and root causes and make recommendations based on risk to the client.

Technical Matrix

This report can be considered a detailed findings matrix targeted to technical staff that will provide more granular detail:

- **Summary:** ERMProtect will provide details specific to the engagement methodology as well as positive security aspects identified.
- **Detailed Findings and Recommendations:** ERMProtect will document the details of all findings, as well as detailed recommendations for remediation per finding/asset and include evidence of controls and information sufficient to replicate/verify the findings. ERMProtect will base recommendations on these root causes and prioritize for a risk-based remediation with an estimation of relative work effort.
- **Artifacts:** ERMProtect will provide details and specific examples, including screenshots, technical details, code excerpts and other relevant observations and also provide documents or data that are relevant but do not fit in other categories.

- **KEY DELIVERABLE: Findings and Recommendations Presentation**

At the end of the project, ERMProtect will facilitate and deliver a formal findings and recommendations presentation to:

- Key Organizational Personnel
- Senior/Top Management

The presentation will summarize the results of each phase of the project, research, evaluation, findings, remediation strategies, and recommendations for remediation and improvement. ERMProtect will cover the full methodology followed during the project as well as advise the organization on how to use the deliverables that ERMProtect will be handing over. This presentation will also serve as an opportunity for the client organization to ask questions. In addition, ERMProtect's team members will always be available both during the project as well as after the project to answer any questions that may arise at any time.

- **PROJECT LEVEL DELIVERABLE: Meetings, Coordination, and Updates**

As part of the project management level deliverables for this project, ERMProtect will conduct weekly status meetings with key stakeholders at the client organization and:

1. Introduce key project team members and define roles and responsibilities
2. Review timelines, meetings, and additional requirements
3. Schedule status meeting and other recurring touchpoints, as required
4. Review engagement progress
5. Identify engagement risks
6. Identify upcoming tasks
7. Request any additional involvement from stakeholders
8. Escalate issues or roadblocks to successful project completion

As a result, ERMProtect will provide the client organization with weekly status update reports highlighting key task area actions, owners, estimated completion dates/times, and overall project status delivered after each meeting.

- **PROJECT LEVEL DELIVERABLE: Knowledge Transfer Session and value-added Services**

Besides delivering the abovementioned reports/deliverables, ERMProtect will provide a session of up to four (4) hours for the transfer of knowledge and training to City of Doral personnel.

We also offer the City of Doral the following value-added services:

✓ One month of free access to ERMProtect Security Awareness Training platform (19 cybersecurity training modules in both English and Spanish).

✓ One phishing attack to all users of the organization.

B. Project Plan

Project Management

ERMProtect's project team will be led by a project manager. The project manager will direct, supervise, and manage a team of cybersecurity experts. This team will include all staff levels including Directors, Managers, Senior Consultants, and Consultants.

Our project management methodology is a time-tested one that incorporates compliance with all requirements that our clients require of us. Our extensive history in providing cybersecurity support to our clients results in our staff being comprised of seasoned, certified, and experienced professionals. We ensure that each contract or task order is well managed and staffed by a certified lead, hands-on and performs the support on-site as required. We utilize PMBOK and other proven processes and best practices to ensure our contracts and tasks comply with client requirements. For all our clients, we ensure we understand and incorporate existing and evolving regulations into our processes and deliverables.

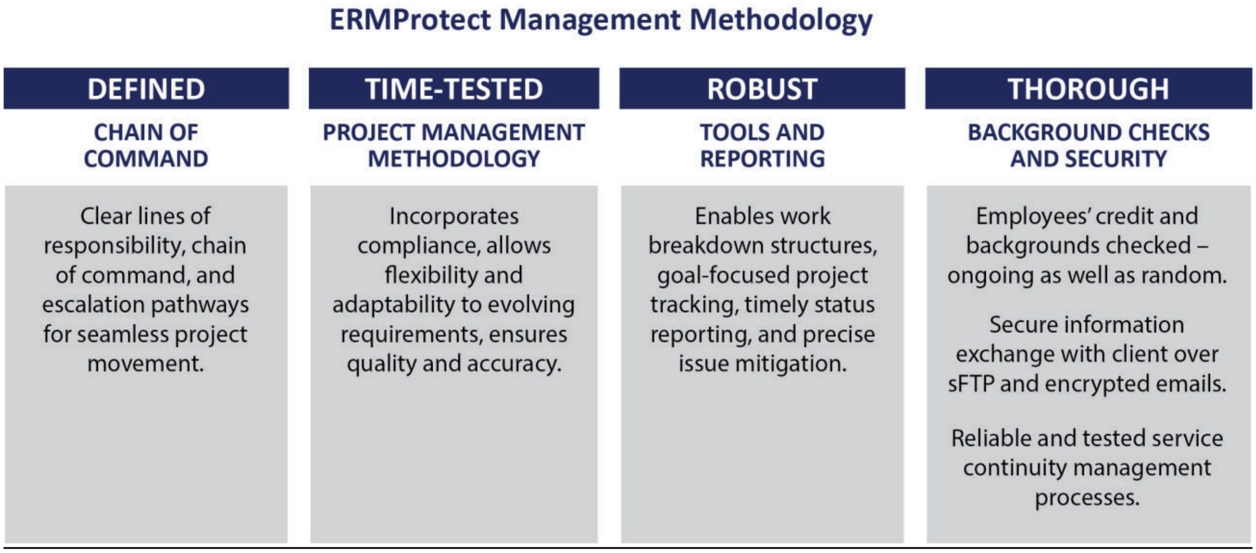
Lines of Responsibility, Authority and Communication

ERMProtect executives are accomplished and seasoned program managers. The Founder and President, Silka Gonzalez, has managed ERMProtect from its inception. This project has the highest levels of corporate commitment to success and Ms. Gonzalez will ensure the project is on schedule, on budget, with the right resources and that the performance represents our excellent history of client satisfaction.

Mr. Esteban Farao, Director of Consulting Services at ERMProtect and our proposed Project Manager for this project will provide the project level day to day oversight to this project. Mr. Farao possesses a strong project and program management background and several years of information security experience with several projects of this nature. He will submit the weekly status reports, deliverables on schedule, and reviews invoices sent to the client as required by contract terms. The report covers all current and planned activities the various teams perform across the tasks and identifies any potential risk or issue areas. Mr. Farao will ensure full compliance and program level management of personnel and is fully able to commit for the company as appropriate to avoid delays. ERMProtect's plan for this project involves several facilitated meetings and discussion sessions. The Project Manager will be the main coordinator and facilitator for all meetings and discussion sessions throughout the project performance period. Mr. Farao will provide project planning and leadership to the entire team. He reports directly to Ms. Gonzalez, has her full support, and is empowered to make decisions regarding day-to-day operations.

Our Operations team will provide the corporate contracts management and administration function for this contract and any resultant task orders. We will ensure full compliance, contract level reporting as needed, and oversee invoice submissions and task management financial functions.

ERMProtect fully recognizes the importance of effective personnel and project management, and we carefully select project managers for key assignments to ensure they have the requisite skills for the job at hand.



ERMProtect Management Methodology

DEFINED	TIME-TESTED	ROBUST	THOROUGH
CHAIN OF COMMAND	PROJECT MANAGEMENT METHODOLOGY	TOOLS AND REPORTING	BACKGROUND CHECKS AND SECURITY
Clear lines of responsibility, chain of command, and escalation pathways for seamless project movement.	Incorporates compliance, allows flexibility and adaptability to evolving requirements, ensures quality and accuracy.	Enables work breakdown structures, goal-focused project tracking, timely status reporting, and precise issue mitigation.	Employees' credit and backgrounds checked – ongoing as well as random. Secure information exchange with client over sFTP and encrypted emails. Reliable and tested service continuity management processes.

The nature of our business is multi-year relationships with clients whereby multiple tasks are issued to address various security issues. Our client retention rate is approximately 90% which illustrates our success in delivering and managing our projects and deliverables with excellent results. Clients return to us time after time and we are able to respond within often short timeframes to address urgent situations. We also have long term contracts with multiple task orders where we adhere to monthly project deliverables and provide performance metrics and quality control.

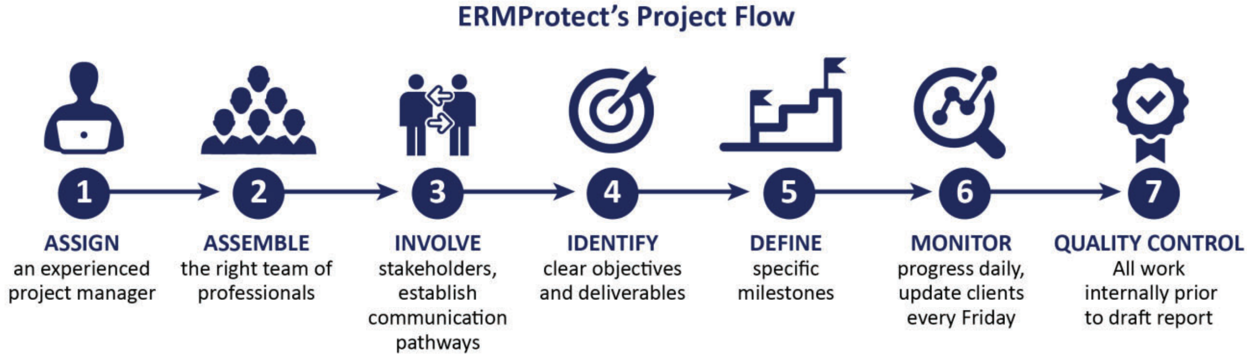
ERMProtect brings a strong, yet flexible program management approach to multi-year projects. Our experience working with clients on intense and rapidly evolving projects has resulted in the development of a scalable project management methodology encompassing the full life cycle of a project including project initiation, planning, executing, monitoring and controlling, and closing out activities and/or programs. In meeting the requirements of this project, our program management strategy will emphasize project planning, quality control, accurate invoicing and reporting, and workload balance throughout project execution.

Our management approach provides cohesive management to all project tasks with staffing occurring both on and off site, avoiding any perception of personal services. It also provides appropriate levels of task management for day-to-day operations.

We will attend task kick-off meetings meeting contract requirements award in person or telephonically as desired by the client. Additionally, we will attend project and task level meetings as needed with appropriate resources attending as necessary. We will meet all task level deliverables and schedules and reporting requirements and submit all required security forms for each employee. We will notify the client immediately when an employee leaves and return their identification card within five (5) days of departure.

Project Flow

ERMProtect will reach out to key personnel and points of contact at City of Doral to introduce our project manager. The project manager will then introduce the project team and provide information on the overall project flow.


ERMProtect's Project Flow
1
ASSIGN
an experienced project manager
2
ASSEMBLE
the right team of professionals
3
INVOLVE
stakeholders, establish communication pathways
4
IDENTIFY
clear objectives and deliverables
5
DEFINE
specific milestones
6
MONITOR
progress daily, update clients every Friday
7
QUALITY CONTROL
All work internally prior to draft report

ERMProtect's project manager will reach out to key client personnel to discuss the project scope, understand the project expectations, objectives, and goals as well as to confirm logistics arrangements, discuss and understand in detail the organization's risk tolerance and culture, and agree upon a communication strategy and plan with escalation channels and specific key individuals identified.

ERMProtect's project manager will then prepare a comprehensive project plan (Work Plan) that covers project timelines, schedules, key individuals involved, rules of engagement, methodology for testing systems, priority ranking of systems, safe/non-production testing time windows, tasks that will be performed as part of the project, listings of information requirements, and deliverables. ERMProtect will then seek City of Doral's review and approval of the project plan before proceeding forward.

If at any moment during the engagement a breach is identified, ERMProtect will notify the City immediately and will pause the security audit until incident response procedures are implemented and the City is no longer affected.

C. Risk Management

ERMProtect's project manager will ensure that risk management is at the forefront of this project. Any project risks ranging from security to performance and delivery will all be kept in check. The "PROJECT MANAGEMENT" section already delved into details of how performance and delivery risks will be kept in check. Let's now discuss security and service continuity related risks below:

Security

ERMProtect will apply strict security measures to all information provided by the client. All Information that can be evaluated internally at the client's locations will be performed on-site at the client and ERMProtect will return all documents (manual and electronic) to the client organization's staff. Final reports and supporting evidence that ERMProtect maintains will be stored in an encrypted format. Moreover, e-mails that contain sensitive information and attachments will be transferred in an encrypted manner.

ERMProtect has implemented robust logical and physical security measures at our site. All client reports and supporting evidence are stored in a secure server and separated by client. Only a limited number of ERMProtect authorized employees have access to the server and clients' resources. Client resources are encrypted while in storage and when they are transmitted to and from clients.

ERMProtect will also use a secure FTP (sFTP) server to exchange sensitive information with the client. The server employs robust security controls including intrusion detection protection, logging, monitoring, and alerting. The sFTP server undergoes ongoing information security testing and reviews to ensure that it complies with industry best practices and leading standards.

Employee Background Checks

It is ERMProtect's policy that all employees will be required to undergo a criminal background check and a credit history check prior to joining the organization. At the time of joining, an employee is screened based on the following procedures:

- Collection of photographs
- Verification of aliases
- Criminal history check
- Credit report check
- Comparison of fingerprints with National and Florida State databases

Additionally, employee backgrounds and credit reports are checked on an ongoing basis as and when required, including, but not limited to, random checks from time to time.

Service Continuity Management

ERMProtect fully recognizes and supports the need for service continuity to its clients in the face of natural disasters/calamities, electrical faults, pandemic outbreaks, non-availability of resources, and/or other such interruptions that threaten the course of normal service provision to our clients.

ERMProtect employs robust data protection strategies in the form of regular backups. Employees backup all data on a central data repository on an ongoing basis. The Security Officer performs a weekly backup of the central repository on a storage drive which is then taken off-site and maintained at a safe contingency location. Full back up recovery testing is performed on a regular basis to ensure that backups are fully restorable. These tests are performed in a test environment that is fully segregated from the production environment. In addition, ERMProtect infrastructural components are protected physically using surge protectors, uninterruptible power supply, multi-level electronic/manual locking, burglar alarms, and fire alarms/extinguishers.

In the event of a natural disaster, ERMProtect will relocate its operations to a safe alternate site. Upon receiving an alert for a natural disaster, ERMProtect management will initiate contingency procedures. The safety of ERMProtect personnel is given foremost importance. All personnel are contacted either physically (if on-site) or by phone to indicate the initiation of contingency procedures. ERMProtect then uses emergency evacuation procedures (if necessary) to evacuate the office premises. In the event that the threat is known in advance, the relocation to the alternate site is done well in advance. An emergency chain of command is followed at all times.

In the event that ERMProtect personnel cannot physically travel (owing to either pandemic or even natural disaster like situations), personnel will work from their home premises and maintain contact over the phone on a regular basis. In such situations, it is likely that clients will not be able to travel as well and hence any information needed shall be coordinated over electronic mediums (such as the Internet or telephonic means).

ERMProtect will transparently communicate and coordinate with all clients during a contingency situation. Collective and cooperative decisions shall be taken on all issues encountered during the course of the contingency.

ERMProtect is available to begin the project almost immediately upon your request. Our project management methods ensure that we keep good with our commitments as far as project milestones are concerned. We have proven past experience in working within client expected timelines and have exceeded client expectations as far as deadlines and project completion milestones are concerned. We also maintain a robust network and coalition with staffing firms and independent consultants who are carefully vetted by us. In the unlikely event that we need to tap into this talent pool, ERMProtect will do so to ensure that project delivery and related schedules do not get adversely impact at any time.

D. Reporting

ERMProtect uses a streamlined and seamless process for progress reporting, communication, and issue escalation.

Reporting, Escalation, and Problem Resolution

The Project Manager will assume full responsibility for preparing meeting agendas, facilitation of sessions, creation and distribution of meeting minutes, and coordination of action items. This will include notifications to meeting attendees, arrangement of meeting facilities, and coordination of any other requisite resources for these meetings and discussion sessions and resultant reports.

The Project Manager will proactively identify risk and when issues materialize will implement agreed upon mitigating strategies to reduce program impact. The Project Manager will provide the day-to-day management of all tasks, functioning as the lead interface with the client point of contact.

The Project Manager has complete access to the ERMProtect executive team and corporate resources as needed and is fully empowered to perform assigned duties. Any issues arising during the performance of the contract will be brought to the attention of the Project Manager. Within 24 hours, if there is no resolution, it will be escalated to the President. We have never had an issue arise that could not be handled at this level to resolve any issues and ensure total and complete customer satisfaction. ERMProtect understands it is our full responsibility to ensure excellent performance, rapid response to issues, and continued work under the contract.

Tools/Reporting

ERMProtect utilizes a work breakdown structure, tools, and time-management/reporting tools to manage and account for contract, task order, and financial tracking and reporting. This allows us to have visibility into task spending levels based on established staffing and schedules. The status of the project and each task will be a topic of each monthly status report. Additionally, weekly status reports addressing each task will be provided and any issues will be presented, and a mitigation plan presented for any involving our tasks. Other deliverables will be defined by final Task Order and provided in the agreed upon format.

Required Forms

Please find the following required forms starting on the next page:

- Solicitation Response Form
- Proposer Qualification Statement
- Bidder/Proposer Affidavits
- Certificate of Authority
- Conflict of Interest Disclosure

Exhibit A – Required Submission Forms

SOLICITATION RESPONSE FORM

City of Doral ITN No. 2024-05
Independent IT Audit Services

Date Submitted	April 2, 2024
Company Legal Name	Enterprise Risk Management, Inc. (dba ERMProtect)
Date of Entity Formation	February 16, 1998
Entity Type (select one)	Corporation / Partnership / LLC / Other: Corporation
Corporate Address	800 S. Douglas Road, Suite 940-N Coral Gables, FL 33134
Office Location	800 S. Douglas Road, Suite 940-N Coral Gables, FL 33134
Taxpayer Identification No.	65-0827427
Authorized Representative (Name and Title)	Silka González - President

1. The undersigned Bidder/Proposer agrees, if this Bid is accepted by the City, to enter into an agreement with the City of Doral to perform and furnish all goods and/or services as specified or indicated in the Contract for the Price and within the timeframe indicated in this proposal and in accordance with the terms and conditions of the Contract.

2. Bidder/Proposer accepts all of the terms and conditions of the Solicitation, including without limitation those dealing with the disposition of Bid Security. This Bid will remain subject to acceptance for 180 days after the day of Bid opening. Bidder/Proposer agrees to sign and submit the Contract with any applicable documents required by this ITN within ten days after the date of City's Notice of Award (If applicable).

3. By responding to this sealed Solicitation, the Bidder/Proposer makes all representations required by the Solicitation and further warrants and represents that Bidder/Proposer acknowledges that it has received and examined copies of the entire Solicitation documents including all of the following addenda:

   Addendum No.: 1 Dated: 03/25/2024 Addendum No.: _____ Dated: __________________

   Addendum No.: 2 Dated: 04/01/2024 Addendum No.: _____ Dated: __________________

   □ Check here If no Addenda were issued by the City.

4. Bidder/Proposer further warrants and represents that it has familiarized themselves with the nature and extent of the Contract, required goods and/or services, site, locality, and all local conditions and applicable laws and regulations that in any manner may affect cost, progress, performance, or furnishing of the Work.

5. Bidder/Proposer further warrants and represents that it has studied carefully all documentation and information provided to the extent applicable to the Work, and has obtained and carefully studied (or assumes responsibility for obtaining and carefully studying) all information provided that pertains to the project or otherwise may affect the cost, progress, performance, or furnishing of the Work, and no additional examinations, investigations, explorations, tests, reports or similar information or data are or will be required by Bidder/Proposer for such purposes.

6. Bidder/Proposer further warrants and represents that it has given the City written notice of all errors or discrepancies it has discovered in the Contract and the resolution thereof by the City is acceptable to Bidder/Proposer.

7. Bidder/Proposer further warrants and represents that this Bid/Proposal is genuine and not made in the interest of or on behalf of any other undisclosed person, firm or corporation; Bidder/Proposer has not directly or indirectly induced or solicited any other Bidder/Proposer to submit a false or sham Proposal; Bidder/Proposer has not solicited or induced any person, firm or corporation to refrain from submitting; and Bidder/Proposer has not sought by collusion to obtain for itself any advantage over any other Bidder/Proposer or over the City.

8. Bidder/Proposer understands that the quantities provided are only provided for proposal evaluation only. The actual quantities may be higher or lower than those in the proposal form.

9. Bidder/Proposer understands and agrees that the Contract Price is Unit Rate Contract to furnish and deliver all of the Work complete in place as such the Proposer shall furnish all labor, materials, equipment, tools superintendence, and services necessary to provide a complete Project.

10. Communications concerning this Proposal shall be addressed to:

Bidder/Proposer: Enterprise Risk Management, Inc. (dba ERMProtect)

Telephone: 305-335-7610

Email Address: sgonzalez@ermprotect.com

Attention: Silka M. Gonzalez

11. The terms used in this response which are defined in the above-referenced Solicitation shall have the meanings assigned to them in such Solicitation.

STATEMENT

I understand that a "person" as defined in 287.133(1)(e), Florida Statutes, means any natural person or entity organized under the laws of any state or of the United States with the legal power to enter into a binding Contract and which Bids or applies to Bid on Contracts for the provision of goods or services let by a public entity, or which otherwise transacts or applies to transact business with a public entity. The term "persons" includes officers, directors, executives, partners, shareholders, employees, members, and agents active in management of the entity.

SUBMITTED THIS 2nd DAY OF April, 2024.

Company Name: Enterprise Risk Management, Inc. (dba ERMProtect)

Company Address: 800 S Douglas Rd. Suite 940 N, Coral Gables, FL 33134

Authorized Representative Signature: Silka Gonzalez

PROPOSER QUALIFICATION STATEMENT

The Proposer's response to this questionnaire will be utilized as part of the City's evaluation to ensure that the Proposer meets, to the satisfaction of the City, the minimum requirements for participating in this Solicitation.

PROPOSER MUST PROVIDE DETAILS FULFILLING THE SOLICITATION'S MINIMUM EXPERIENCE REQUIREMENTS IN THE FORM BELOW. IT IS MANDATORY THAT PROPOSERS USE THIS FORM IN ORDER TO INDICATE THAT THE MINIMUM EXPERIENCE REQUIREMENT IS MET. NO EXCEPTIONS WILL BE MADE.

Proposer	Enterprise Risk Management, Inc. (dba ERMProtect)		
Years in Business	26 years		
Years of Experience Providing Independent IT Audit Services	26 years		
Project No. 1			
Project Name:	Cybersecurity Risk Assessment / Penetration Tests		
Project Description:	Five (5) year contract providing various cybersecurity services including digital forensic, all types of penetration tests (external, internal, wireless, web application, segmentation), PCI QSA services and Security Risk Assessment based on the SP 800-30 r1 "Guide for Conducting Risk Assessments" using the NIST Cybersecurity framework (CFS) 1.1 as a control baseline. ERMProtect was just awarded the next six(6) year contract for $699,829 to provide the same services.		
Budget/Cost:	$469,126 (approximately)	Contract Dates:	Jan 2019 - Dec 2024
Owner/Client Name:	Miami Dade County	Reference Name:	Lars Schmekel
Reference Phone No.:	305-596-8779	Reference Email:	lars.schmekel@miamidade.gov
Project No. 2			
Project Name:	Technical Security Audit / Comprehensive Security Assessment / Penetration Tests		
Project Description:	Performed various tecnical security audits, security implementations and developed policies and procedures. Performed various penetration tests including external, internal, wireless networks and web applications. Work for the City for more than 6 years.		
Budget/Cost:	$80,100	Contract Dates:	Sep 2023 / present (in progress)
Owner/Client Name:	City of West Palm Beach	Reference Name:	Paul Jones
Reference Phone No.:	561-578-2420 / 561-822-1258	Reference Email:	pjones@wpb.org
Project No. 3			
Project Name:	Digital Forensic / PCI DSS Audits / Security Trainings and Phishing Tests		
Project Description:	The scope of work includes digital forensic services, a yearly PCI DSS audits, external,internal, web application and segmentation penetration testing. ERMProtect also conducted tailored security awareness training sessions for various groups including IT professionals, general staff, ad executives. Work for the City for more than 8 years.		
Budget/Cost:	$176,088	Contract Dates:	Nov 2019 - Dec 2024
Owner/Client Name:	City of Coral Gables	Reference Name:	Nelson Gonzalez
Reference Phone No.:	305-460-5076 / 786-525-5851	Reference Email:	ngonzalez@coralgables.com

Exhibit A – Required Submission Forms

BIDDER/PROPOSER AFFIDAVITS

Business Name: Enterprise Risk Management, Inc.

D.B.A.: ERMProtect Federal I.D. No.: 65-0827427

Business Address: 800 S. Douglas Road, Suite 940-N

City: Coral Gables State: FL Zip: 33134

I, the undersigned affiant do swear and affirm that I am an authorized agent of the above-named business ("Bidder") and authorized to make the following statements and certifications on Bidder's behalf:

1. Ownership Disclosure

Pursuant to City Code Section 2-384, the above-named Bidder hereby discloses the following principals, individuals, or companies with five percent (5%) or greater ownership interest in Bidder (supplement as needed):

Name	*Address*	*% Ownership*
Silka González	800 S. Douglas Road, Suite 940-N Coral Gables, FL 33134	95%
Esteban Farao	800 S. Douglas Road, Suite 940-N Coral Gables, FL 33134	5%

The above-named Bidder hereby discloses the following subcontractors (supplement as needed):

Name	*Address*	*% Ownership*
N/A		

Bidder hereby recognizes and certifies that no elected official, board member, or employee of the City of Doral ("City") shall have a financial interest in any transactions or any compensation to be paid under or through any transactions between Bidder and City, and further, that no City employee, nor any elected or appointed officer (including City board members) of the City, nor any spouse, parent or child of such employee or elected or appointed officer of the City, may be a partner, officer, director or proprietor of Bidder, and further, that no such City employee or elected or appointed officer, or the spouse, parent or child of any of them, alone or in combination, may have a material interest in the Bidder. Material interest means direct or indirect ownership of more than 5% of the total assets or capital stock of the Bidder.

Any exception to these above-described restrictions must be expressly provided by applicable law or ordinance and be confirmed in writing by City. Further, Bidder recognizes that with respect to any transactions between Bidder and City, if any Bidder violates or is a party to a violation of the ethics ordinances or rules of the City, the provisions of Miami-Dade County Code Section 2-11.1, as applicable to City, or the provisions of Chapter 112, part III, Fla. Stat., the Code of Ethics for Public Officers and Employees, such Bidder may be disqualified from furnishing the goods or services for which the bid or proposal is submitted and may be further disqualified from submitting any future bids or proposals for goods or services to City. The term "Bidder," as used herein, include any person or entity making a proposal herein to City or providing goods or services to City.

2. Public Entity Crimes

1. Bidder is familiar with and understands the provisions of Section 287.133, Florida Statutes
2. Bidder further understands that a person or affiliate who has been placed on the convicted Bidder list following a conviction for a public entity crime may not submit a bid, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a bid, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit bids, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for CATEGORY TWO for a period of 36 months following the date of being placed on the convicted Bidder list.
3. Based on information and belief, the statement which I have marked below is true in relation to the entity submitting this sworn statement. (**INDICATE WHICH STATEMENT APPLIES**.)
    - ___✓___ Neither the entity submitting this sworn statement, nor any of its officers, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, nor any affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989.
    - _______ The entity submitting this sworn statement, or one or more of its officers, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, or an affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989.
    - _______ The entity submitting this sworn statement, or one or more of its officers, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, or an affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989. However, there has been a subsequent proceeding before a Hearing Officer of the State of Florida, Division of Administrative Hearings and the Final Order entered by the Hearing Officer of the State of Florida, Division of Administrative Hearings and the Final Order entered by the Hearing Officer determined that it was not in the public interest to place the entity submitting this sworn statement on the convicted Bidder list. (Attach a copy of the final order.)

3. Compliance With Foreign Entity Laws

Applicant certifies as follows:

a. Bidder is not owned by the government of a foreign country of concern, as defined in Section 287.138, Florida Statutes.
b. The government of a foreign country of concern does not have a controlling interest in Bidder, as defined in Section 287.138, Florida Statutes.
c. Bidder is not organized under the laws of a foreign country of concern, as defined in Section 287.138, Florida Statutes.
d. Bidder does not have a principal place of business in a foreign country of concern, as defined in Section 287.138, Florida Statutes.
e. Bidder is not on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in Iran Terrorism Sectors List, created pursuant to s. 215.473.
f. Bidder is not engaged in business operations in Cuba or Syria.
g. Bidder is not participating in a boycott of Israel, and is not on the Scrutinized Companies that Boycott Israel list in accordance with the requirements of Sections 287.135 and F.S. 215.473, Florida Statutes

4. Disability, Nondiscrimination, and Equal Employment Opportunity

Applicant certifies that Bidder is in compliance with and agrees to continue to comply with, and ensure that any subcontractor, or third party contractor under any and all contracts with the City of Doral complies with all applicable requirements of the laws listed below including, but not limited to, those provisions pertaining to employment, provision of programs and services, transportation, communications, access to facilities, renovations, and new construction.

- The American with Disabilities Act of 1990 (ADA), Pub. L. 101-336, 104 Stat 327, 42 USC 1210112213 and 47 USC Sections 225 and 661 including Title I, Employment; Title II, Public Services; Title III, Public Accommodations and Services Operated by Private entities; Title IV, Telecommunications; and Title V, Miscellaneous Provisions.
- The Florida Americans with Disabilities Accessibility Implementation Act of 1993, Section 553.501 553.513, Florida Statutes.
- The Rehabilitation Act of 1973, 229 USC Section 794.
- The Federal Transit Act, as amended 49 USC Section 1612.
- The Fair Housing Act as amended 42 USC Section 3601-3631

5. Conformance with OSHA Standards

Applicant certifies and agrees that Applicant has the sole responsibility for compliance with all the requirements of the Federal Occupational Safety and Health Act of 1970, and all State and local safety and health regulations, and in the event the City engages Bidder, Bidder agrees to indemnify and hold harmless the City of Doral, against any and all liability, claims, damages losses and expenses the City may incur due to the failure of itself or any of its subcontractors to comply with such act or regulation in the performance of the contract.

6. E-Verify Program Affidavit

Affiant certifies the following:

a. Affiant is familiar with and understands the provisions of Section 448.095, Florida Statutes and 48 CFR 52.222-54 and has sufficient knowledge of the personnel practices of the Bidder to execute this Declaration on behalf of the Bidder.
b. Bidder has registered with and utilizes the federal work authorization program commonly known as E-Verify or any subsequent replacement program, in accordance with the applicable provisions and deadlines established in F.S. 448.095, which prohibits the employment, contracting or sub-contracting with an unauthorized alien.
c. Bidder does not knowingly employ Affiants or retain in its employ a person whose immigration status makes them ineligible to work for the Bidder.
d. Bidder has verified that any subcontractors utilized to deliver goods or services to the City through the Contractor's contract with the City use the E-Verify system and do not knowingly employ persons whose immigration status makes them ineligible to work for the subcontractor. The undersigned further confirms that it has obtained all necessary affidavits from its subcontractors, if applicable, in compliance with F.S. 448.095, and that such affidavits shall be provided to the City upon request.
e. Failure to comply with the requirements of F.S. 448.095 may result in termination of the Bidder's contract(s) with the City of Doral.

7. No Contingency Affidavit

Affiant certifies the following:

a. Neither Bidder nor any principal, employee, agent, representative or family member has promised to pay, and

Bidder has not and will not pay, a fee the amount of which is contingent upon the City of Doral awarding a contract.

b. Bidder warrants that neither it, nor any principal, employee, agent, or representative has procured, or attempted to procure, a contract with the City of Doral in violation of any of the provisions of the Miami- Dade County conflict of interest and code of ethics ordinances.

c. Bidder acknowledges that a violation of this warranty may result in the termination of any contracts and forfeiture of funds paid, or to be paid, to the Bidder if awarded a contract.

8. Copeland Anti-Kickback Affidavit

Affiant certifies that no portion of any sums will be paid to any employees of the City of Doral, its elected officials, or its consultants, as a commission, kickback, reward or gift, directly or indirectly by Bidder or any member of Bidder's firm or by any officer of the corporation in exchange for business with the City of Doral.

9. Non-Collusion Affidavit

I, the undersigned affiant, swear or affirm that:

a. Affiant is fully informed respecting the preparation and contents of the attached Bid/Proposal by Contractor and of all pertinent circumstances respecting such Bid/Proposal.

b. Such Bid/Proposal is genuine and is not a collusive or sham Bid/Proposal.

c. Neither the said Contractor nor any of its officers, partners, owners, agents, representatives, employees or parties in interest, including Affiant, have in any way colluded, conspired, connived or agreed, directly or indirectly, with any other firm or person to submit a collusive or sham Bid/Proposal in connection with the Work for which the attached Bid/Proposal has been submitted; or to refrain from bidding in connection with such Work; or have in any manner, directly or indirectly, sought by agreement or collusion, or communication, or conference with any firm or person to fix any overhead, profit, or cost elements of the Bid/Proposal or of any other person submitting a response to the solicitation, or to fix any overhead, profit, or cost elements of the quoted price(s) or the quoted price(s) of any other bidding/proposing person, or to secure through any collusion, conspiracy, connivance, or unlawful agreement any advantage against the City or any person interested in the proposed Work.

d. The price(s) quoted in the attached Bid/Proposal are fair and proper and are not tainted by any collusion, conspiracy, connivance, or unlawful agreement on the part of the Contractor or any other of its agents, representatives, owners, employees or parties in interest, including this Affiant.

10. Drug Free Workplace Program

Bidder, in accordance with Florida statute 287.087 hereby certifies that the Bidder does all of the following:

a. Publishes a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the workplace and specifying the actions that will be taken against employees for violations of such prohibition.

b. Informs Employees about the dangers of drug abuse in the workplace, the business' policy of maintaining drug-free workplace, any available drug counseling, rehabilitation, and employee assistance programs, and the penalties that may be imposed upon employees for drug abuse violations.

c. Gives each employee engaged in providing the commodities or contractual services that are under bid a copy of the statement specified in subsection (a).

d. In the statement specified in subsection (a), notifies the employees that, as a conditions of working on the commodities or contractual services that are under bid, the employee will abide by the terms of the statement and will notify the employer of any conviction of, or plea of guilty or nolo contendere to, any violation of chapter 893 or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction.

e. Imposes a sanction on, or require the satisfactory participation in, a drug abuse assistance or rehabilitation program if such is available in the employee's community, by any employee who is so convicted.

f. Makes a good faith effort to continue to maintain a drug-free workplace through implementation of this section.

□ Select here if Not Applicable

11. Cone of Silence Certification

Affiant certifies and that Affiant has read and understands the Cone of Silence" requirements set forth in this Solicitation and further certify that neither I, nor any agent or representative of the Company has violated this provision.

BIDDER AFFIRMATION

I, the undersigned affiant, being first duly sworn as an authorized agent of the below-named Bidder, does hereby affirm and attest under penalty of perjury as the proposed Bidder for City of Doral that the certifications and statements provided above on behalf of Bidder are true to the best of affiant's knowledge and belief and that Bidder is compliant with all requirements outlined in these City of Doral Affidavits. Bidder acknowledges it is required to comply with and keep current all statements sworn to in the above affidavits and will notify the City of Doral immediately if any of the statements attested hereto are no longer valid.

Enterprise Risk Management, Inc. (dba ERMProtect)
Bidder Name

Silka M. Gonzalez 03/25/2024
Date Signed

Affiant Signature

President SILKA M. GONZÁLEZ
Affiant Name & Title (Printed)

STATE OF Florida
COUNTY OF Marion

The foregoing instrument was affirmed, subscribed, and sworn to before me this 25th day of March, 2024 by means of ☒ physical presence or □ online notarization, by Silka Gonzalez who is personally known to me or who produced the following identification: Drivers License.

[Notary Seal]

Notary Public State of Florida
Sunita Singh
My Commission HH 464705
Expires 11/15/2027

Notary Public for the State of FL
My commission expires: 11/15/2027

CERTIFICATE OF AUTHORITY

(IF CORPORATION OR LLC)

I HEREBY CERTIFY that at a meeting of the Board of Directors of ERMPROTECT, a corporation organized and existing under the laws of the State of FLORIDA, held on the 25 day of MARCH 2024, a resolution was duly passed and adopted authorizing SILKA GONZALEZ (Name) as PRESIDENT (Title) of the corporation/company to execute agreements on behalf of the corporation/company and providing that their execution thereof, attested by the secretary of the corporation/company, shall be the official act and deed of the corporation/company. I further certify that said resolution remains in full force and effect.

IN WITNESS WHEREOF, I have hereunto set my hand this 25 day of MARCH, 2024.

Secretary Signature: Silka M. Gonzalez

Print Name: SILKA M. GONZALEZ

STATE OF Florida
COUNTY OF Marion

The foregoing instrument was affirmed, subscribed, and sworn to before me this 25th day of March, 2024 by means of ☒ physical presence or □ online notarization, by Silka Gonzalez who is personally known to me or who produced the following identification: Drivers License.

[Notary Seal]

Notary Public State of Florida
Sunita Singh
My Commission HH 464705
Expires 11/15/2027

Notary Public for the State of FL
My commission expires: 11/15/2027

CONFLICT OF INTEREST DISCLOSURE

Business Name: Enterprise Risk Management, Inc.

D.B.A.: ERMProtect Federal I.D. No.: 65-0827427

Business Address: 800 S. Douglas Road, Suite 940-N

City: Coral Gables State: FL Zip: 33134

Please note that all business entities interested in or conducting business with the City are subject to comply with the City of Doral's conflict of interest policies as stated within the certification section below. If a vendor has a relationship with a City of Doral official or employee, an immediate family member of a City of Doral official or employee, the vendor shall disclose the information required below.

1. No City official or employee or City employee's immediate family member has an ownership interest in vendor's company or is deriving personal financial gain from this contract.
2. No retired or separated City official or employee who has been retired or separated from the City for less than one (1) year has an ownership interest in vendor's Company.
3. No City employee is contemporaneously employed or prospectively to be employed with the vendor.
4. Vendor hereby declares it has not and will not provide gifts or hospitality of any dollar value or any other gratuities to any City employee or elected official to obtain or maintain a contract.

Conflict of Interest Disclosure*	
Name of City of Doral employees, elected officials, or immediate family members with whom there may be a potential conflict of interest: None __________ __________	( ) Relationship to employee ( ) Interest in vendor's company ( ) Other (please describe below) __________ __________ (✓) No Conflict of Interest

**Disclosing a potential conflict of interest does not automatically disqualify vendors. In the event vendors do not disclose potential conflicts of interest and they are detected by the City, vendor will be exempt from doing business with the City.*

I certify that this Conflict-of-Interest Disclosure has been examined by me and that its contents are true and correct to my knowledge and belief and I have the authority to so certify on behalf of the Vendor by my signature below:

Silka González	March 22,2024	Silka González
Signature of Authorized Representative	Date	Printed Name of Authorized Representative

Appendix: ERMProtect Team Resumes

Please find the resumes starting on the next page

SILKA GONZALEZ

President & Founder

sgonzalez@ermprotect.com
305-447-6750

EDUCATION

Master's in accounting information systems - Florida International University

Entrepreneurial Master's Program - Massachusetts Institute of Technology

Bachelor of Science, Computer Information Systems - Xavier University

Bachelor of Arts, Accounting - Xavier University

CERTIFICATIONS

- Certified Public Accountant (CPA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Information Technology Professional (CITP)
- Certified in Risk and Information Systems Control (CRISC)
- PCI Qualified Security Assessor (QSA)
- NACD Board Leadership Fellow
- Chainalyis Cryptocurrency Fundamentals Certification (CCFC)

Summary

Silka Gonzalez is president of ERMProtect. She founded the company in 1998 after a distinguished career as an IT executive for Fortune 500 companies and two Big Four accounting firms. A pioneer in the information security field, Silka foresaw the need to combine professionals with IT security, data regulation, and IT audit backgrounds to properly serve the cybersecurity industry. Since, 1998, her company has grown to provide Information Security and IT risk management services to more than 450 clients in over 35+ industries worldwide, including 60 clients in banking and finance.

Silka started her career in IT consulting at Arthur Young. Subsequently, she was a manager of IT and business services at Price Waterhouse, Manager of Information Systems Auditing for Diageo PLC, and CISO for American Bankers Insurance Group (now Assurant Solutions).

Relevant Experience

- Silka oversees a 25-person cybersecurity firm that has been in business since 1998 providing information security, IT audit, digital forensics, security regulatory compliance and security awareness training.
- Silka has kept ERMProtect at the forefront of cybersecurity trends and positioned the company as a trusted advisor to large firms and organizations, including FP&L, ADT, Ryder Systems, Norwegian Cruise Lines, USPS, DOD, DeCA, Department of Homeland Security, Miami Dade County, Perry Ellis International, the state of New Hampshire, and the Metropolitan Washington Airports Authority.
- Silka early on aimed the company's services to banks and community banks, which were one of the first industries required by regulators to have information systems security plans, controls, and audits. Her clients include many large U.S.-regulated banks in the U.S., Latin America, and Europe.
- Silka has established credibility and trust in the marketplace for her boutique firm by instituting a hiring model that emphasizes impeccable academic credentials, multiple high-level certifications, proven experience at respected U.S. firms, and a high-level of integrity.
- Silka and her team are recognized as subject matter experts in the field of information security. She is frequently interviewed by news media (NBC, CBS, Telemundo, Univision, Miami Herald). She regularly speaks at banking, legal, and minority professional associations, and has presented with DOJ computer crime experts.

ERMProtect
Cybersecurity Solutions

ESTEBAN FARAO

Director, IT Consulting Services

efarao@ermprotect.com
305-447-6750

EDUCATION

Bachelor's degree in Information Systems, Universidad be Belgrano.

Master's degree in Management Information Systems, Universidad de Salvador

Master's degree in International Business, Florida International University

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Chief Information Security Officer (C|CISO)
- Certified Ethical Hacker (CEH)
- Payment Card Industry Professional (PCIP)
- PCI-Qualified Security Assessor (PCI-QSA)
- EnCase Certified Examiner (EnCe)
- Certified Network Defense Architect (CNDA).
- Certified Data Privacy Solutions Engineer (CDPSE)
- PCI Forensic Investigator (PFI)

Summary

Esteban Farao is a Director of IT Consulting Services. He performs computer forensics and incident response during major security breaches. As an expert certified ethical hacker, he knows the routes malicious actors use to penetrate organizations and puts this knowledge to use to protect clients. His deep knowledge of computer forensics has helped him break open major cases related to fraud, embezzlement, IP theft and other misdeeds. He is also an expert in assisting organizations to prepare, plan and respond to data breaches.

Experience

With two master's degrees and 25+ years in information security, Esteban has led >10k projects related to general data breaches, PCI DSS-related data breaches and investigative forensics. He has served as the court-appointed "neutral" in disputes, testified in both U.S. and Latin American courts, and provided evidence to the United States Secret Service and other enforcement agencies. He has performed thousands of gap assessments for clients related to data compliance, including for PCI DSS, GLBA, SEC, NIST, FISM, HIPAA, HITECH, etc.

Prior to joining ERMProtect, Esteban led attack and penetration testing assignments for PwC in London and set up and managed the company's IT security practice in Argentina. He holds 11 high-level IT Security certifications.

Case Highlights

- **Security Training and Table-Top Exercises –** Prepared and delivered table-top exercise training for institutions such as Helm Bank USA and the State of Kansas, Office of the Bank Commissioner.
- **Digital Forensics -** Extracted information from various mobile phones to provide evidence for a large sports investigation case related to use of illegal substances.
- **Law Firm Support –** Extracted information from various servers, computers, mobile devices, and mobile phones to provide evidence that executives committed corporate fraud.
- **Data Breach –** Determined that a bank employee copied a database to run a large identity theft operation.
- **PCI Data Breach –** As PCI PFI, investigated multiple large breaches of credit card data affecting all major payment cards brands and retailers processing from $1.5M-$17M monthly.
- **Forensic Investigation –** Determined who processed $2 million dollars of unauthorized wire transfer transactions via an on-line banking system by installing a malicious program in the administrator's machine.

AKASH DESAI

Director, Information Security Consulting Services

adesai@ermprotect.com
305-447-6750

EDUCATION

Master's degree in Information Networking with a Cybersecurity specialization from Carnegie Mellon University

Bachelor's degree in Computer Science from Sardar Patel University

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Ethical Hacker (CEH)
- PCI Qualified Security Assessor (PCI-QSA)
- Payment Card Industry Professional (PCIP)

Summary

Akash Desai is a Director of Information Security Consulting Services for ERMProtect. For more than 20 years, he has combined technical expertise with creativity and problem-solving acumen to create solutions that address challenging cybersecurity problems. He leads penetration tests, comprehensive security assessments, gap analyses, and incident response tests and reviews to identify and fix vulnerabilities. To address human vulnerabilities, he developed ERMProtect's security awareness training practice which offers off-the-shelf and customized training for employees using animations, games, mini lectures, etc. His customized training for large federal agencies helped improve security of the military supply chain and of U.S. immigration and citizenship records worldwide and at U.S. embassies. Prior to joining ERMProtect, Akash worked for two years with the Computer Emergency Response Team Coordination Center (CERT®/CC) where he evaluated security attacks on U.S. private enterprise and provided solutions to prevent them.

Relevant Experience

- **Security Awareness Training –** Mr. Desai is the brain behind ERMProtect's security awareness training. He developed scripts for a 75+ library of animations, games, videos, and mini-videos available on our LMS or in SCROM-compliant modules. He has developed highly customized training for:
  - **NAVAIR** – Personnel involved in the supply chain to enable them to securely purchase weaponry, jets, ships, vehicles, and critical parts to supply the U.S. military.
  - **USCIS** – Personnel with access to sensitive citizenship and immigration data of the U.S. government and embassies.
  - **The Gap** – Employees of a global retail company to help protect the company's infrastructure systems and data.
  - **Penn State University** – 100,000 users to teach them to spot attacks and adhere to information security policies.
  - **Norwegian Cruise Lines** – Employees to protect data on and offshore and to ensure compliance with regulations.

- **Penetration Testing –** Developed and led penetration testing in complex environments, followed by remediation. For banks, compromised accounts, wire transfer systems, and physical cameras. *Sample clients: Telecommunications giant, many banks, large hospital, global insurance company, states of New Hampshire and West Virginia.*

- **Security Incident Response & Data Breach** – Developed, tested, and improved security incident response plans for many clients. Helped a City ward off a developing cybersecurity incident that involved a takeover of servers, workstations, devices, and key systems to mine bitcoin.

POOJA KOTIAN

Manager, Information Security Consulting Services

pkotian@ermprotect.com
305-447-6750

EDUCATION

Bachelor's degree in Engineering, Information Technology - Sardar Patel University

CERTIFICATIONS

- Infosys Quality Foundation (Internal to Infosys)
- Dotnet Technology 101 (Internal to Infosys)
- STAR Certification (Internal to Infosys)

ERMProtect
Cybersecurity Solutions

Summary

Pooja Kotian is a Senior Information Security Consultant at ERMProtect. She has more than 12 years of experience as a Senior Systems Engineer and as an Information Security Consultant overseeing penetration testing and vulnerability assessments, performing regulatory compliance assessments, reviewing policies and procedures related to IT security, and developing comprehensive security training content. She began her career as a Systems Engineer for Infosys before joining ERMProtect in 2015. She is highly experienced at conducting penetration tests of various kinds of web applications, internal and external networks, mobile applications, and social engineering. She performs vulnerability assessments on systems, applications, and infrastructures to identify, classify and prioritize vulnerabilities. She performs audits to ensure adherence to best practices and applicable laws, standards, and regulations.

Relevant Experience

- **Penetration Testing –** Found difficult-to-identify vulnerabilities in web applications, mobile applications, APIs, and network infrastructures. *Sample Clients: Assurant Solutions, State of New Hampshire, Safra National Bank of New York, City of Boynton Beach, and Metropolitan Washington Airport Authority.*
- **Vulnerability Assessments:** Identified highly technical security weaknesses with the help of scans, manual tests, as well as deep-dive source code reviews. Provided detailed remediation recommendations to clients and helped follow-through efforts. *Sample Clients: Segpay, Banco do Brasil, City of Coral Gables, CSID – Experian, and City of Lake Worth Beach.*
- **Security Assessments –** Performed comprehensive security assessments that helped clients comply with various regulations and regulatory requirements including PCI DSS, GLBA, FACTA, GDPR, FedRAMP, FISMA, ISO 27001, FFIEC, etc. *Sample Clients: itelBPO, Outplex, Helm Bank, Bancredito, SlimCD.*
- **Security Training –** Developed innovative information security training content used to train client employees on a vast array of cybersecurity awareness topics. *Sample Clients: CentralReach, Bancredito, Axiomatic, Banco de Credito del Peru, and Norwegian Cruise Line.*
- **Social Engineering –** Performed several social engineering assessments including phishing, spear phishing, impersonation, etc. to help clients test the cybersecurity awareness levels of their employees. Provided recommendations for improvement. *Sample Clients: Baer's Furniture, Safrapay, Welligent, and City of Lake Worth Beach.*

ERMProtect
Cybersecurity Solutions

DIVYANSH ARORA

Manager, Information Security Consulting Services

darora@ermprotect.com
412-708-6331

EDUCATION

Bachelor's degree in Technology, Computer and Communication, Manipal Institute of Technology

Master's degree in Information Technology – Information Security, Carnegie Mellon University

CERTIFICATIONS

- Offensive Security Certified Professional

AWARDS

- EPT Leaderboard – 20+ machines vs. 5 teams
- CMU Academic Scholarship, 2019
- 2You Rock – Awarded for organizing PwC One Cyber Bootcamp, 2018

Summary

Divyansh Arora is a Consultant, Information Security Services for ERMProtect. Prior to receiving his master's degree in Information Technology at the prestigious Carnegie Mellon University, Divyansh worked as a Senior Cybersecurity Analyst at PricewaterhouseCoopers. At PwC, he conducted hundreds of vulnerability assessments of web applications, IPs in the network, Android & iOS mobile applications and IoT devices such as CCTV and Central Command displays, for multiple government and private clients. He also assessed various phases in the SDLC and performed static and dynamic source code reviews. Subsequently, while working on his master's degree, he worked as an intern at McKinsey & Company, researching cloud security. After graduating with a 3.79 GPA, he joined ERMProtect to provide a wide variety of IT security services.

Relevant Experience

- **Vulnerability Assessment & Penetration Testing –** Conducted vulnerability assessment and penetration testing of 100+ web applications, millions of IPs in the network, over 20 Android & iOS mobile applications and IoT devices such as Spy Cameras, Baby Monitors, CCTV, Central Command Displays, for multiple government and private clients to ensure the security of critical infrastructure from various threat actors. Discovered possibility of fraud payments in payment gateway applications and prevented significant monetary losses to the client.

- **Security Awareness Training –** Delivered social engineering attack prevention training to 1500+ employees of the client by executing official phishing campaign, achieving a 65% success rate by developing a fake website to obtain sensitive information.

- **Secure Code Review –** Performed static and dynamic secure code review of various web, desktop and mobile applications developed in multiple languages, using a number of tools such as AppScan, Fortify, Coverity.

- **Built Cloud-Native SIEM tool –** Built a Scalable Cloud-Native SIEM (Security Information & Event Management) System based on AWS to help collect and aggregate logs, detect incidents, and respond to security threats.

- **Security Training and Table-Top Exercises –** Participated in preparing and delivering table-top exercise training for institutions such as Helm Bank USA and the State of Kansas, Office of the Bank Commissioner.

COLLIN CONNORS

Consultant, Information Security Consulting Services

cconnors@ermprotect.com
305-447-6750

EDUCATION

Bachelor's degree in Mathematics and Computer Science, University of Miami

Ph.D. in Computer Science, University of Miami (May 2025)

GPA: 3.80

Summary

Collin Connors is an ERMProtect Information Security Consultant. He develops the company's proprietary tools, such as our automated phishing and phishing-detection tools. He oversees the company's internal security to prevent attacks on our networks, utilizing penetration testing, monitoring logs and security software, including vendor software that analyzes our metadata to assess potential compromises. A Ph.D. candidate at the University of Miami, he is researching the use of AI to detect malware, implementation of blockchain at banks, and prevention of attacks in a shared cloud environment.

Relevant Experience

- **Penetration Tests** - Performed Internal, External, Wireless and Web application penetration tests for clients and for ERMProtect to secure infrastructure, systems, and data. Created automated tools to improve test performance.
- **Security Incident Response** – Participated on a team of security directors to create, implement, and test a plan to prevent attacks on ERMProtect's internal networks, including monitoring for malware, adding security measures, and performing simulated attacks.
- **Security Monitoring** – Created an internal security program to monitor logs for security threats. Researched multiple security tools and implemented the tools into the ERMProtect security architecture. Supervised the continued monitoring of security logs and response to detected threats.
- **Policies and Procedures** – Designed and wrote all internal security policies and procedures based on industry best practices. Oversaw testing and implementation of these policies and procedures.

Research

- **Blockchain Architecture -** Designed a novel blockchain architecture for use in general applications. The architecture was designed to be highly module and easy for a user to implement. Implemented our novel architecture to show the efficacy of our architecture.
- **A Deep Learning Approach to Malware Detection -** Created over 20 deep learning models to analyze Portable Executable Files and classify them as malicious or benign**.** Compared the various architectures to find the most efficient and most accurate model, and then looked at the information measure of each model to validate of our findings.

ERMProtect
Cybersecurity Solutions

AVIRAL SHARMA

Consultant, Information Security Consulting Services

asharma@ermprotect.com
(206)513-9143

EDUCATION

Bachelor's degree in Technology, Computer Science and Engineering - Specialization in Information Security, Vellore Institute of Technology

Master's degree in Information Technology – Information Security – Applied Advanced Study, Carnegie Mellon University

Summary

Aviral Sharma is a Consultant, Information Security Services, for ERMProtect. He performs risk assessments, data compliance assessments, and penetration testing for the company. Aviral received his master's degree in information technology from the prestigious Carnegie Mellon University, where he underwent advanced training in code reviews, digital forensics, and vulnerability assessments for mobile applications. He is experienced in web development, image processing, and machine learning as a software developer. He graduated from Carnegie Mellon with a 3.6 GPA, and during his time at Carnegie, worked as an intern at various startups such as Intros.ai and TreeMama Organization as a web developer and an information security analyst. At ERMProtect, in addition to providing a wide variety of IT security services to clients, he is also pursuing certifications in digital forensics and cryptocurrency tracing to further enhance his cybersecurity investigation skills.

Relevant Experience

- **Risk Assessments –** Conducted risk assessments such as GLBA, FACTA for multiple clients. Participated in various vulnerability assessments and penetration tests conducted by ERMProtect. Discovered and proved the lack of security awareness among the non-technical employees of a client's staff, paving the way for training that prevented significant potential monetary losses to the client.

- **Cyber Forensics investigations –** As part of the capstone project for Cyber Forensics Specialization, Aviral had the opportunity to be trained in Cyber forensics and participate in mock investigations that mirrored real-world security incidents. These team investigations were conducted in conjunction with industry experts including but not limited to professionals from cyber forensics teams at police departments, law firms, and private investigation companies, etc.

- **Vulnerability Assessments –** Performed static and dynamic secure code reviews as well as vulnerability assessments of web and mobile applications developed in multiple languages, using a number of tools such as AppScan, Fortify, Coverity.

- **Research Experience –** Published a thesis exploring the feasibility of using Digital Twins concept to reinforce the security, availability, and privacy of an IT infrastructure with meaningful returns.

- **Web Development & Security –** Working on development of a SOC2 automation tool as a full-stack developer at ERMProtect. Has experience in using various tools such python, Java, JavaScript, php, MySQL, etc.

ERMProtect
Cybersecurity Solutions

VIBHA DHIRAJ PUTHRAN

Information Security Consultant

vputhran@ermprotect.com
305-447-6750

EDUCATION

Bachelor in Technology (Computer Science Engineering), PES University

Postgraduate Diploma in Cyber Law and Cyber Forensics, National Law School of India University

Master of Science in Information Technology – Information Security, Carnegie Mellon University

CERTIFICATIONS

- EC Council Certified Incident Handler
- Microsoft Azure Fundamentals
- CyberArk Certified Trustee
- Splunk 7. X Fundamentals Part 1
- Autopsy and Cyber Triage DFIR
- ICSI Certified Network Security Specialist (CNSS)

Summary

Vibha Dhiraj Puthran is an Information Security Consultant. She performs digital forensic investigations and data breach investigations for the firm's diverse client base. Her training in incident response and advanced digital forensics equips her to battle data breaches in a technically and legally-sound manner. She has assisted multiple organizations to identify system vulnerabilities, harden security, and close gaps that could lead to breaches and regulatory fines. Prior to joining ERMProtect, she worked as a Cybersecurity Consultant for PwC in India. She has a master's degree in information technology from Carnegie Mellon University.

Relevant Experience

- **Digital Forensic & Incident Response** – Led investigations involving data manipulation by an insider, ATM intrusions, ransomware, business email compromises, and other types of data breaches.
- **Tabletop Exercises** – Led tabletop drills for multinational clients to test and improve their incident response plans. Created an Incident Response Playbook and facilitated training.
- **Cyber Crime** – Working as an intern for a State Police department, gained an understanding of the methodology of investigation of cybercrimes reported to the Government of India. Learned the digital forensics methodology, including acquiring hard drive images and analysis of call detail records. Also, co-led training for police officers regarding cybercrimes.

Publications

- **Data Privacy and User Consent** – An Experimental Study on Various Smartphones (2021) International Journal of Digital Society (IJDS), Volume 12, Issue 1
- **Detecting Data Exfiltration on Android Phones (2020)** – Presented the paper at the World Congress on Internet Security (WorldCIS) 2020 Conference held in London.

EXHIBIT “B”

Fee Schedule

All Forensic work including regular forensic tasks, depositions, and court testimony	$250 per hour
All Other Consulting Services – Senior Level	$225 per hour

The above hourly rates shall be adjusted on an annual basis by three percent (3%) per year.

RESOLUTION No. 24-122

A RESOLUTION OF THE MAYOR AND THE CITY COUNCIL OF THE CITY OF DORAL, FLORIDA, APPROVING THE AWARD OF INVITATION TO NEGOTIATE ITN #2024-05 FOR "INDEPENDENT IT AUDIT SERVICES" TO ENTERPRISE RISK MANAGEMENT, INC., AS THE TOP-RANKED PROPOSER; AUTHORIZING THE CITY MANAGER TO NEGOTIATE AND EXECUTE AN AGREEMENT WITH THE TOP-RANKED PROPOSER, AND TO EXPEND BUDGETED FUNDS IN CONNECTION THEREWITH; FURTHER AUTHORIZING THE CITY MANAGER TO NEGOTIATE AND ENTER INTO AN AGREEMENT WITH THE NEXT HIGHEST RANKED PROPOSER SUCCESSIVELY IF AN AGREEMENT CAN NOT BE NEGOTIATED WITH THE TOP-RANKED PROPOSER; AND PROVIDING FOR AN EFFECTIVE DATE

WHEREAS, the City of Doral ("City") Council directed the Interim City Manager to conduct a competitive procurement to engage an independent IT auditing firm to conduct a forensic analysis of the City's IT security systems, with a focus on folder permissions within the City's network file shares; and

WHEREAS, on March 6, 2024, the City of Doral issued Invitation to Negotiate ("ITN") No. 2024-05 inviting all qualified and experienced firms specializing in IT security audits, digital forensics, and penetration testing to submit proposals and notices were posted on the City's website, VendorRegistry.com, and Demandstar.com; and

WHEREAS, all questions of a material nature were answered via two (2) addenda posted on March 25, 2024 and April 1, 2024 on the City's website, VendorRegistry.com, and Demandstar.com; and

WHEREAS, on April 10, 2024, the City received and opened six (6) timely proposals, five (5) of which were deemed responsive; and

WHEREAS, an Evaluation Committee was convened on April 24, 2024 via publicly-noticed meeting, and all responsive firms were invited for presentations; and

WHEREAS, the Evaluation Committee was reconvened for presentations from all responsive proposers on April 25, 2024; and

WHEREAS, the Evaluation Committee was reconvened for final evaluations on April 29, 2024 via publicly-noticed meeting; and

WHEREAS, the Evaluation Committee ranked Enterprise Risk Management, Inc. as the top-ranked proposer; and

WHEREAS, the City Manager recommends that the City Council award the ITN to Enterprise Risk Management, Inc. and authorize the Interim City Manager to negotiate and execute an agreement for Independent IT Audit Services; and

WHEREAS, the City Manager further recommends that the City Council authorize the City Manager to negotiate and enter into an agreement with the next highest ranked proposer successively if an agreement cannot be negotiated with the top-ranked Proposer.

NOW THEREFORE, BE IT RESOLVED BY THE MAYOR AND THE CITY COUNCIL OF THE CITY OF DORAL AS FOLLOWS:

Section 1. **Recitals.** The above recitals are confirmed, adopted, and incorporated herein and made a part hereof by this reference.

Section 2. **Approval.** The award of ITN No. 2024-04 for Independent IT Audit Services to Enterprise Risk Management, Inc. is approved. If an agreement cannot be negotiated with the top-ranked Proposer, the City Council approves the award of ITN

No. 2024-04 for Independent IT Audit Services to the next highest ranked proposer successively until an agreement is negotiated and executed as specified below.

<u>Section 3.</u> **<u>Authorization.</u>** The City Manager is authorized to negotiate and execute an agreement with Enterprise Risk Management, Inc. in a form acceptable to the City Attorney. The City Manager is further authorized to negotiate and enter into an agreement with the next highest ranked proposer successively if an agreement cannot be negotiated with the top Proposer. The City Manager is further authorized to expend budgeted funds as provided for herein.

<u>Section 4.</u> **<u>Implementation.</u>** The City Manager and the City Attorney are hereby authorized to take such further action as may be necessary to implement the purpose and provisions of this Resolution.

<u>Section 5.</u> **<u>Effective Date.</u>** This Resolution shall become effective immediately upon its adoption.

The foregoing Resolution was offered by Councilmember Porras who moved its adoption. The motion was seconded by Councilmember Pineyro and upon being put to a vote, the vote was as follows:

Mayor Christi Fraga	Yes
Vice Mayor Oscar Puig-Corve	Yes
Councilwoman Digna Cabral	Yes
Councilman Rafael Pineyro	Yes
Councilwoman Maureen Porras	Yes

PASSED AND ADOPTED this 8 day of May, 2024.

CHRISTI FRAGA, MAYOR

ATTEST:

CONNIE DIAZ, MMC
CITY CLERK

APPROVED AS TO FORM AND LEGAL SUFFICIENCY
FOR THE USE AND RELIANCE OF THE CITY OF DORAL ONLY:

GREENSPOON MARDER, LLP
INTERIM CITY ATTORNEY