

5/2/2023

Statement of Work

Iowa K-12 Schools

Vulnerability Management
w Risk Assessment v 1.0



Prepared by
Martin Yarborough
Martin Yarborough and Associates LLC

Table of Contents

Table of Contents	2
Overview and Shared Objectives	3
Project Scheduling	3
Project Scope and Definition	3
Deliverables	6
Assumptions and Customer Responsibilities.....	6
Change control process	8
Martin Yarborough & Associates Personnel Skills and Qualifications.....	9
Termination	12
Pricing	12
Signature and Acceptance.....	13

SAMPLE

Statement of Work for Vulnerability Scanning with Cybersecurity Risk Assessment

This Statement of Work (“SOW”) is between Martin Yarborough & Associates (“Company”) and Iowa Schools (“Customer”) for the services described in the SOW (individually, the “Service” or collectively, the “Services”) and is effective as of the date last executed in the Signature section below.

Overview and Shared Objectives

Customer has requested Martin Yarborough & Associates to provide a Statement of Work and pricing for the implementation of Vulnerability Scanning:

The objectives of the engagement are:

1. Document CIS/NIST Security Framework Controls
2. Conduct monthly vulnerability scans
3. Conduct phishing simulations (2)
4. Perform penetration testing (not more than 6 endpoints)

Project Scheduling

Martin Yarborough and Associates provides a high-level project plan as part of this SOW.

Project Scope and Definition

Pre-Engagement

1. The customer signs the Statement of Work and provides a purchase order number and returns to myarb@martinyarborough.com.
2. MYA generates and invoice from the SOW and sends to the engagement sponsor.
3. Engagement sponsor provides payment for the subscription.
4. Upon receipt of payment, MYA provides the Vulnerability Pre-Engagement Worksheet to the Sponsor.
5. MYA prepares secure portal (BaseCamp) for deliverables.
6. The Sponsor completes and submits the Pre-Engagement Worksheet to MYA.
7. MYA schedules 2 conference calls:
8. Sponsor Orientation (30 min)
9. Single Point of Contact (SPOC) Orientation (30 min)
10. MYA conducts Sponsor orientation call. (1 hour)
 - a. Introduces the process

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

- b. Discusses Communication
 - c. Describes the CIS Control Review
 - d. Describes electronic network assessment methodology
 - e. Describes phishing simulations
 - f. Describes penetration testing
 - g. Describes the Deliverables
 - h. Identified the Stakeholders
11. MYA conducts the SPOC orientation call. (1 hour)
- a. Introduces the process
 - b. Describes the contents of the SPOC packet
 - c. Discovery
 - d. WMI procedure
 - e. Windows firewall procedure
 - f. Describes electronic network assessment methodology
 - g. Describes the CIS Control Review
 - h. Describes electronic network assessment methodology and vulnerability scanning
 - i. Describes phishing simulations
 - j. Describes penetration testing
 - k. Discuss the monthly vulnerability meetings (dates/times)
12. MYA provides a final project plan to the Sponsor upon completion of the SPOC orientation.
13. Sponsor needs to approve final project plan for engagement to proceed.
14. MYA provides vulnerability scanner to SPOC via USPS for installation. (Assistance is provided)

Workshop

1. SPOC invites identified stakeholders to a Kickoff Workshop.
2. MYA prepares for workshop.
3. MYA conducts workshop.

Assess

1. Discovery
 - a. SPOC downloads the Discovery spreadsheet from the BaseCamp portal.
 - b. SPOC and team complete the Discovery and upload to the BaseCamp portal. This document identifies the exact hosts to be scanned and authentication credentials to be used.
2. CIS Control Review
 - a. SPOC schedules 6 interviews (1 hr.) with selected stakeholders:
 - 1) Data review
 - 2) Network review
 - 3) User review
 - 4) Program review
 - 5) Device review
 - 6) Applications review
 - b. MYA sends calendar invites to all stakeholder participants.
 - c. MYA posts interview questions on BaseCamp portal.

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

- d. MYA conducts CIS Review
3. Electronic Vulnerability Assessments
 - a. MYA provides the vulnerability assessment tool to the SPOC for installation and configures for network and vulnerability studies (see requirements below).
 - b. MYA conducts a network assessment from information provided in the Discovery document. (5–6 days)
 - c. MYA conducts an external vulnerability assessment on all external-facing hosts from information provided in the Discovery. (5–6 days)
 - d. MYA conducts an internal vulnerability assessment on all internal hosts from information provided in the Discovery. (8–10 days)
 - e. MYA continues the vulnerability assessments monthly for 12 consecutive months.
4. Phishing Simulations
 - a. MYA receives a list of email candidates to participate in the Phishing simulation.
 - b. MYA prepares pre-training material in the form of an infographic.
 - c. SPOC sends the infographic to all employees.
 - d. MYA prepares the phishing simulator.
 - e. MYA generates the phishing email.
 - f. MYA generates the phishing landing page.
 - g. MYA generates the phishing remedial page.
 - h. MYA conducts a pilot run with selected IT staff members.
 - i. MYA corrects any issues with the pilot run.
 - j. MYA starts the phishing simulation and allows to run for 10 days.
 - k. MYA disengages the phishing simulator and extracts the resulting metrics (including emails and names of those who got “phished”).
5. Penetration Testing
 - a. Following the initial vulnerability scan, MYA will recommend to the customer a list of potential endpoints that should be pen tested.
 - b. MYA will perform an Nmap scan of the suggested endpoints.
 - c. MYA will perform a deep vulnerability scan of the suggested endpoints.
 - d. MYA will perform a Metasploit scan of the suggested endpoints.
 - e. MYA will attempt to circumvent and exploit the suggested endpoint if possible.
 - f. MYA generates reporting of the process and end results and provides them to the customer within the BaseCamp portal.

Develop

1. CIS Control Review
 - a. MYA documents and disaggregates all information provided in the CIS Control review.
 - b. MYA conducts a risk assessment on all data.
 - c. MYA calculates the overall security maturity of the customer and provides comparisons.
 - d. MYA generates impact statements and provides recommendations for remediation.

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

2. Electronic Assessment Reports
 - a. Monthly reports (12 months) (technical)
 - b. Quarterly reports (overview)
 - c. MYA reviews all of the electronic scan results and generates a table of identified vulnerabilities, risk factors and suggested mitigations.
3. Phishing Simulation
 - a. MYA disaggregates all data and provides reporting to the customer along with findings, impacts and recommendations for additional training.
 - b. The process is repeated for all who “failed” the phishing simulation to assess the effectiveness of remedial training.
4. Penetration Testing
 - a. MYA disaggregates all Nmap, OpenVAS and Metasploit data and manually attempts to circumvent the endpoint.
 - b. All documentation is maintained in a secure portal for review. Findings, impacts and recommendations are generated.

Present

1. MYA provides DRAFT deliverable documents to the Sponsor/SPOC via a secure portal at regular intervals defined in the project plan.
2. MYA established a date/time for the Sponsor/SPOC review of the deliverables.
3. MYA conducts the review.
4. MYA modified the deliverables based on input from the Sponsor.

Post-Engagement

1. MYA provides the Sponsor electronic copies of all FINAL deliverables.
2. MYA provides the Sponsor with a URL to complete a customer satisfaction survey.
3. Sponsor completes and submits the survey.
 - a. Any mitigations are discussed and immediately resolved to the customer’s satisfaction.
4. The project is closed.

Deliverables

Item	Description	Format
1	Security Framework Control Review with recommendations	PDF
2	Monthly Electronic Scanning Results	PDF
4	Phishing Simulation Report with recommendations	PDF
5	Pen Test Results with recommendations	PDF

Assumptions and Customer Responsibilities

Assumptions:

The Company may make certain assumptions while specifying the Services and deliverables detailed in this SOW. It is the Customer’s responsibility to identify any incorrect assumptions or take immediate action which

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

will make all of the Company’s responsibility to identify any incorrect assumptions or take immediate action which will make all of the Company’s assumptions correct. Martin Yarborough & Associates has made the following specific assumptions while specifying the Services detailed in this SOW:

1. If the assumptions used to develop the SOW are found to be incorrect, the parties agree to meet and negotiate, in good faith, equitable changes to the SOW, Service Levels and/or Fee Schedule, as appropriate.
2. The prices for the Services are based on Customer’s environment as known by the Company at the time of execution of this SOW. If the volumes, consumption factors or requirements change by plus or –5 (5%) percent, the county will adjust the pricing to reflect these changes.
3. The resources to perform the Services shall be available (including any travel time) Monday through Friday, 8:00 AM to 5:00 PM local Customer time (excluding nationally observed holidays, based on a forty (40) hour week, unless previously agreed upon between Customer and Company.
4. The Company reserves the right to perform portions of the work remotely according to a schedule mutually agreed to by both Customer and Company.
5. A typical schedule involves working remotely at least one business day per week to complete deliverables and/or any applicable documentation. Additional fees may apply for travel/Services outside of this timeframe.
- 6.
7. The Company is not responsible for resolving compatibility or other issues that cannot be resolved by the manufacturer or for configuring hardware or software in contradiction to the settings supported by the manufacturer.
8. The Company is not responsible for project or Service delivery delays caused by Customer facility or personnel challenges.
9. Completing transition within the agreed timeframe is contingent upon the Company receiving the necessary Customer information and gaining access to the necessary Customer resources, personnel and facilities in a timely manner.
10. The Company’s pricing does not assume the responsibility of any Customer or third-party personnel, hardware, software, equipment or other assets currently utilized in the Customer’s operating environment.
11. The Company reserves the right to sub- contract portions of all of the requested Services with permission from the Customer.

Not Included with This Service:

1. Any services or activities other than those specifically noted in this SOW and identified in a mutually signed Work Order.

Customer Responsibilities

Both Customer and Company are responsible for collaborating on the execution of the Services. The Company’s responsibilities have been set forth elsewhere in this SOW. Customer agrees generally to cooperate with Company to see that the Services are successfully completed. Customer agrees to the following assigned responsibilities:

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

1. Prior to the start of this SOW, Customer will indicate to Company in writing a person to be the single point of contact, according to the project plan, to ensure that all tasks can be completed within the specified time period. All Services communications will be addressed to such point of contact (the “Customer Contact”). Failure to do so might result in an increase in project hours and/or length in schedule.
2. Customer will provide technical points-of-contact, who have a working knowledge of the enterprise components to be considered during the Services (“Technical Contacts”). The Company may request that meetings be scheduled with Technical Contacts.
3. The Customer Contact will have the authority to act for the Customer in all aspects of the Service including bringing issues to the attention of the appropriate persons within Customer’s organization and resolving conflict in requirements.
4. The Customer Contact will ensure that any communication between Customer and Company, including any scope-related questions or requests, are made through the appropriate Company Project Manager.
5. The Customer Contact will provide timely access to technical and business points of contact and required data/information for matters related to the scope of Service.
6. The Customer Contact will ensure attendance by key Customer contacts at Customer meetings and deliverable presentations.
7. The Customer Contact will obtain and provide project requirements, information, data, decisions and approvals within one working day of the request, unless both parties agree to a different response time.
8. Customer may be responsible for developing or providing documentation, materials and assistance to Company and agrees to do so in a timely manner. Company shall not be responsible for any delays in completing its assigned tasks to the extent that they result from Customer’s failure to provide such timely documentation, materials and assistance.
9. The Customer Contact will ensure the Services personnel have reasonable and safe access to the Project site, a safe working environment, an adequate office space, and parking as required.
10. Customer will inform Company of all access issues and security measures and provide access to all necessary hardware and facilities including VPN access to the vulnerability scanner.
11. Customer is responsible for providing all hardware, software, telephone Internet access, and facilities in a timely manner for the successful completion of the Services. Facilities and power must meet Company’s requirements for the products and Services purchased.
12. Customer agrees to complete a customer satisfaction survey.

Change control process

- The “Change Control Process” is the process that governs changes to the scope of the Services during the term of this SOW. The Change Control Process will apply to new Services components and to enhancements of existing services.
- A written “Change Order” will be the vehicle for communicating any desired changes to the Services. It will describe the proposed changes to the Services scope, pricing, resources, tasks, and deliverables; the reason for the change; related assumptions and Customer responsibilities; and the schedule and price impacts of the change. The Company Project Manager will draft the Change Order document

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

based on discussions with Customer and Company team. Only changes included in a Change Order signed by both Customer and Company will be implemented.

- In some cases, a Change Order will authorize Company to study the impacts of proposed change will have in terms of required changes to Services scope, schedule, and price. If, upon completion of the study, Customer agrees to proceed with an identified scope change, the Company Project Manager will draft a separate Change Order to detail the specifics associated with that change.

Martin Yarborough & Associates Personnel Skills and Qualifications

The Company, will, at its sole discretion, determine the number of personnel and the appropriate skill sets necessary to complete the Services. Customer understands that Company resources may include employees of Company and/or a service provider or subcontractor to Company. Company personnel may work on-site at Customer location or off-site inside at a Company or other location as determined by the needs of the Services and by specific agreement of the Customer project manager. Company has identified the following initial resource levels for these Services. Key responsibilities for the resources are identified below.

Martin Yarborough

Career Summary

For three decades Martin Yarborough has been involved in public education as a teacher, Director of Technology, Dean of Technology, Chief Technology Officer, and lastly, as the Chief Information Officer of the Fort Worth Independent School District, the fourth largest school district in Texas. This life-long Texan and seasoned educational professional received his Masters' degrees in Educational Administration and Curriculum and Instruction from Tarleton State University in Stephenville Texas and Bachelors' degrees in Chemistry and Biology from the same institution with doctoral work in Instructional Technology from the University of North Texas and Northern Illinois University.

Recognizing the potential of technology as a teaching and learning tool, Mr. Yarborough brought the Glen Rose public schools into educational technology prominence in 1982 by implementing the very first district-wide fiber-optic LAN in Texas, thus beginning a life-long love affair with educational technology that exists to this day. An innovator in implementing cutting edge, efficient technology into schools, Martin was among the first to implement voice over IP into classrooms, provide teachers with corporate-style email, develop a project-management practice to oversee large-scale, district-wide technology implementations, and incorporate extensive use of distance learning and professional development into public school classrooms.

His experience extends into application software development as well as management of large implementations of PeopleSoft, Computer Associates, and Microsoft deployments to include ERP products, network monitoring tools, email systems, K-12 ERATE, and portal environments. Martin was instrumental in the establishment of a comprehensive data warehouse and longitudinal data system for the Fort Worth public schools incorporating all benchmark and other testing data with student demographics in a SharePoint environment for access by faculty and staff through portal technologies.

Mr. Yarborough is a sought-after speaker on topics ranging from better efficiencies through assessments and educational practices as well as cybersecurity and disaster recovery.

Areas of Expertise

- **End User Computing** and client deployment strategies to include workstation management, output devices, and messaging practices (e-mail, instant messaging, voicemail, and fax).
- **Data Center Analysis and Design** to include server and server platforms including virtualization, storage (SAN, NAS and DAS), facilities management, backup/restore practices, and disaster recovery.

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

- **Application Enablement** to include business ERP, enterprise application software, software development lifecycles.
- **Security and Vulnerability** to include intrusion detection, account management and security assessments.
- **Services Management** to include service desk operation, change management practices, release management practices, problem management, and incident management. **Specialist in Business Impact Studies, Risk Analysis and Disaster/Recovery Planning.**

Project Experience

- **Medium City Government** – Conducted an IT Assessment and facilitated a strategic plan to expand the IT program to accommodate a large sporting event venue to be constructed within the city limits.
- **Large Professional Organization in California** – Facilitated a state-wide strategic plan for a large organization of IT professionals
- **Large Educational Service Center in California** - Served as Senior Consultant in the Disaster/Recovery planning development. The 6 week engagement resulted in a comprehensive metric identification practice through the evaluation of a Business Impact Analysis, Risk Assessment and Application Analysis. The evaluation led to the implementation of a Disaster/Recovery program for the organization to span 16 weeks.
- **Medium Utility District in Florida** - Served as Senior Consultant in the Disaster/Recovery planning development. The 8 week engagement resulted in the development of 8 application recovery plans, a server recovery program, a network recovery plan and a telecommunication program.
- **Medium University in Texas** – Served as Senior Consultant in the Disaster/Recovery planning development. The 6 week engagement resulted in a comprehensive metric identification practice through the evaluation of a Business Impact Analysis, Risk Assessment and Application Analysis. The evaluation led to the development of an Educational Contingency Plan as well as a DR/BC plan for the college.
- **Large public school district in Virginia** – Served as project manager on an enterprise assessment making 15 actionable recommendations which resulted in a complete re-design of the service desk environment and desktop support. Six transformational follow-on engagements ensued.
- **Large public transportation company in South** – Served as Project Director on an assessment to review plans for a secondary disaster/recovery site for the largest roadway project in Texas. The results were detailed recommendations for implementing a self-contained data center that could temporarily be located in a remote location and moved in the event of a disaster. The assessment engagement led to data center consolidation and transformation opportunities.
- **Large public school district in South** – Provided project leadership on the largest assessment to date of the second largest school district in Texas. The new CIO was struggling making decisions and putting business cases together to request additional budget. A complex, custom assessment was developed with intent to review budget, hardware and services in preparation for an ITO proposal. The result was praised by the CIO, CFO and Superintendent and the adoption of the assessment by the School Board serving as the basis for an on-going strategic planning effort.
- **Medium school district in the Heartland** – Worked with the superintendent of schools to conduct an extensive Educational Assessment. Results included recommendations to move ERP, Messaging and Network Services to a cloud delivered model. The district retained my services for a 24-month period to assist the organization in implementing the recommendations. I established a comprehensive PMO Framework and trained the staff on project management during the implementation. The result was a complete data center transformation. This was an acquisition account for my company and as a result of the relationships I established, they have been one of the highlights of this past year. The organization was selected as a case study. This included the pm of a GroupWise/Exchange migration, conversion from Novell to MS Active Directory, implementation of video conferencing as well as several staff augmentations using 3rd party vendors to assist in the implementation of an extensive wireless network.
- **Medium school district in the Heartland** – Conducted a 4 week assessment of the IT Enterprise to include end-user computing, services management, data center operations and security and vulnerability. Identified 15 core initiatives and provided an operational roadmap for remediation. The result was an 18-month staff-augmentation as the interim CIO engaged to implement the suggested
- initiatives. The first step was the development of a PMO framework and staff training to implement the PMO.
- **State Government** – Conducted an enterprise technology assessment focusing on Administrative Applications, Web Operations and IT Infrastructure and Operations. Identified 12 core initiatives for transformation and submitted statements of work to deliver the transformational consulting. This included extensive leadership augmentation.
- **Large school district in South** – Fort Worth Texas – Provided the leadership to conduct an evaluation of ERP and Student Information Systems for transformation of the accounting practices of the district. Supervised the bidding and procurement

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

process for the business ERP environment and let the implementation and migration practice for the successful implementation of Tyler Technologies MUNIS program.

- **Large school district in South** – Served in an interim CIO capacity to project manage a “botched” PeopleSoft implementation. I was able to bring the payroll system into compliance in less than 3 months and implement the benefit system.
- **Large school district in South** – Served as project manager for the conversion of a legacy ERP to a full PeopleSoft implementation. This involved the hiring of technical/functional consultants, procurement of equipment including bidding and supervising staff during this phase. The effort resulted in a successful implementation in less than 6 months of Financials/HR/Benefits and Payroll including self-service.
- **Large municipal government in South** – Conducted an enterprise technology infrastructure assessment. Engagement spanned 12 weeks of effort. Identified 14 core initiatives for improvement. Developed extensive roadmap for implementation. Follow-on included the implementation of a full-scale PMO and the training of staff to utilize the PMO framework as well as Novel • Microsoft conversions and data center transformations.
- **Large school district in West** – Evaluated infrastructure capacity leading toward 15 week engagement for an enterprise technology infrastructure assessment. Worked with technology staff to identify 12 primary initiatives toward improvement of core infrastructure to include end user management, service management, data center operations and security. Effort resulted in a storage transformation and key network transformations.
- **Large school district in South** – Worked with Superintendent and CIO to implement a comprehensive infrastructure assessment. Effort spanned 15 weeks and resulted in the development of 15 core initiatives focusing on data center, end-user and service management.
- **Large University in South** – Conducted a readiness assessment of classroom multimedia infrastructure. Effort resulted in an organizational re-design and re-organization to consolidate siloed IT programs into a centralized IT department and let to extensive consulting engagements post-ITSA.
- **Large University in West** – Conducted an enterprise technology assessment focusing on Administrative Applications, Web Operations and IT Infrastructure and Operations. Identified 15 core initiatives for transformation and submitted statements of work to deliver the transformational consulting. This included extensive leadership augmentations, ITIL training and data center transformation.
- **Medium University in South** – Served as project manager on an ERP/Student Information conversion from a legacy mainframe system to a Unix platform running on Alpha processors. Conversion took 4 months plus another 3 months to convert over 1MM transcript records into the new format. Conducted University-wide staff development to faculty and staff on the use of the new ERP/SIS environment and established process and procedure for the management of the system.

Professional Qualifications

Education

- B.S. Biology, Tarleton State University, 1979
- B.S. Chemistry, Tarleton State University, 1979
- M.Ed. Education Administration, Tarleton State University, 1990.
- Ph.D Instructional Technology, Northern Illinois University, 2001

Certifications

- Lifetime Teaching Certificate, Texas, 1979
- Mid-Management Administrative Certificate, Texas, 1990
- Superintendent Certificate, Texas, 1990
- PMP, 2007
- ITIL v.3, 2008
- TOGAF v.9, 2011
- Certified Ethical Hacker, 2013

Presentations and Publications

- T.H.E. Journal Publication – Author... “A Journey Across the Fiber”, 1984.
- Educause Presentation – Speaker ...“Assessment for Efficiency”, 2008.
- ISTE Presentation – Keynote... “Designing a Better Educational Data Center”, 1996.

SOW – Vulnerability Management w Risk Assessment – Iowa Schools

- TechSig Presentation – Keynote... “Outsourcing Data Center Practices”, 1992.
- SETL Presentation – Keynote... “Why Assessments Work”, 2010.
- ATLE Presentation – Keynote... “How to Increase Efficiency in your Data Center”, 2011.
- ASCD Presentation – Speaker... “Integrating classroom computers in to the curriculum”, 1996.
- MISA Presentation – Keynote... “Creating a climate of Efficiency in the Data Center”, 2013.
- SETL Presentation – Facilitator ... “Cloud Computing and BYOD”, 2013

Termination

Customer may terminate this SOW for convenience upon providing Company with thirty (30) days written notice. Upon any termination of this SOW or the associated Agreement, Customer shall pay all of Company’s unpaid fees and out-of-pocket expenses accrued to the effective date of such termination. If Customer fails to perform any payment obligations hereunder and such failure remains un-remediated for fifteen (15) days, Company may suspend its performance until payment is received or terminate this SOW and the associated Agreement upon written notice.

Pricing

Pricing is provided as a subscription fee. Payment must be received before services can commence.

SAMPLE

Signature and Acceptance

By signature below, Customer and Martin Yarborough and Associates acknowledge and agree to this statement of work (SOW).

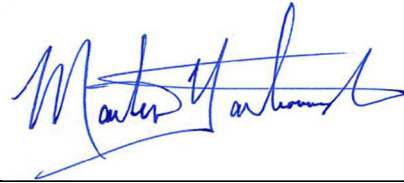
Client Contact Signature

Printed Name

Title

Company Name

Date



Martin Yarborough and Associates Contact Signature

Martin Yarborough

Printed Name

Principal Consultant

Title

Martin Yarborough and Associates LLC

Company Name

May 2, 2023

Date

Please fax a copy of this signed SOW (with all pages in full) to 1-817-887-3371 or scan/email to myarb@martinyarborough.com.

SAMPLE

Quote

Follows on the next page

SAMPLE