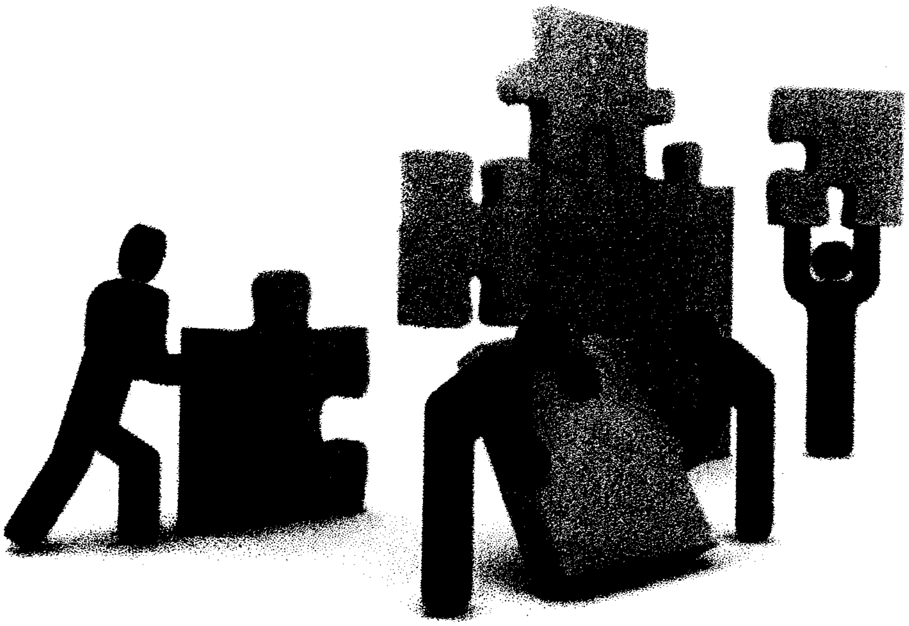
Assero Security



Statement of Work for:

Johnson County

Presented to:

Dan Milam

Information Security Review

October 2013
Version 1.0

Presented by:
Doug Landoll

Assero Security

Dan Milam
Information Technology Director
Johnson County, TX

Mr. Milam,

Assero Security is pleased to respond to your inquiry into our services. This proposal describes our Information Security Review service, which provides customers with an independent review of their information security controls.

Once signed this document serves as a Statement of Work (SOW) and sets forth an agreement between Assero Security and Johnson County.

We look forward to working with you to address your security concerns.

Doug Landoll
CEO, Assero Security
10800 Pecan Park Blvd.
Suite 250D
Austin, TX 78750

Assero Security is an Austin-based information security consultancy specializing in information security assessments and compliance. Assero Security consultants have provided information security and compliance services to State, Local, Educational Entities, Hospitals, Insurance Companies, and Commercial Organizations. Our experience with the information security regulations and security assessment techniques, and information security systems allows us to provide effective and efficient information security assessment services ensuring the success of your project. A brief outline of some of our expertise and experience is listed below:

Customer		Project
	State of Arizona, Department of Administration	**FISMA Security Policy and Standards**: Worked directly with the State CIO and State CISO to develop the security policy and standard set applicable to all Arizona State agencies.
TxDMV	Texas Department of Motor Vehicles	**TAC202 Gap Assessment:** Performed a security assessment of Texas DMV security controls against the Texas Administrative Code (TAC) 202 (Security Controls) to support their security program development and TAC 202 compliance.
TEXAS WORKFORCE COMMISSION	Texas Workforce Commission	**FISMA Gap, Security Plan, and Security Risk Assessment:** Performed a FISMA Gap Assessment on the Texas Workforce Commission systems to obtain compliance with the US Department of Labor requests for FISMA compliance. Included the development of a System Security Plan and a Security Risk Assessment.
coaers	City of Austin Employee's Retirement System	**Security Controls Assessment:** Performed an assessment of existing security controls for the City of Austin Employee's Retirement System to support their completion of external security surveys.
AUSTIN COMMUNITY COLLEGE DISTRICT	Austin Community College District	**ISO Gap Assessment:** Performed an ISO 27002 Gap Assessment and physical controls review for Austin Community College District to support their security program development.
TEXAS A&M UNIVERSITY CORPUS CHRISTI	Texas A&M Corpus Christi	**ISO / TAC202 Gap Assessment:** Performed a security assessment of Texas A&M Corpus Christi Campus security controls against the Texas Administrative Code (TAC) 202 and ISO 27002 to support their security program development and TAC 202 compliance.
Tarrant County College District	Tarrant County College District	**Physical Security Risk Assessment:** Performed a security assessment of physical security controls planned for the downtown campus of Tarrant County College District to support the planning of the new campus.
UH	University of Houston	**PCI Gap Assessment:** Performed a PCI Gap Assessment for University of Houston to support their security program development and PCI compliance.
TML Intergovernmental Employee Benefits Pool	Texas Municipal League Intergovernmental Employee Benefits Pool	**HIPAA Gap Assessment and Risk Assessment:** Performed a HIPAA Gap Assessment and Security Risk Assessment for Texas Municipal League (IEBP) to support their security program development and HIPAA compliance.

The Assero Difference

Assero Security specializes in information security assessment engagements. There is a vast difference in the skill sets it takes to review or assess security controls and the skills it takes to lead an organization to improvements necessary to become compliant. Assero security consultants not only understand security technology but how to interpret information security regulations for your organization.

Assero security is a leader in the INFOSEC community in the development of assessment methodologies and the training of INFOSEC professionals. The RIOT (Review, Interview, Observe, Test) data gathering approach, introduced in "The Security Risk Assessment Handbook' [Landoll 2006, 2010] has been adopted throughout the industry and Mr. Landoll has taught over 200 classes in information security topics including CISSP Exam Prep.

Assero security is uniquely qualified to address the needs of the [customer] in the Information Security Review.

Statement of Work

1 Background

Johnson County has identified a need for a Information Security Review. Assero Security offers a comprehensive solution with its Information Security Review service.

Assero Security offers a pragmatic approach to Information Security Reviews based on industry best practices and assessment approaches outlined in "The Security Risk Assessment Handbook" [Landoll 2006, 2010]. Our Security Program Review service is designed to effectively review your existing security controls for against industry best practices.

2 Scope of Services

Security Program Review

This service addresses the customer's request for an independent third-party to assess the effectiveness of the current information security controls. The proposed information security review will evaluate the customer's current administrative, physical, and technical controls for compliance with the industry best practices.

Assero Security

Project Initiation

- Kickoff Conference Call
- Documentation Request
- Onsite and Interview Scheduling

KICKOFF CONFERENCE CALL Assero Security will schedule a phone call with the customer to review the statement of work, project approach, and project assumptions. The customer POC is required on this call but others interested in the project may attend.

DOCUMENTATION REQUEST Assero Security will send the customer POC a documentation request for all relevant documents (e.g., policies, procedures, standards, network maps, and relevant audit reports) for the engagement. These documents shall be collected and sent to the Assero Security consultant with adequate time to be reviewed prior to the onsite portion of the engagement (typically one week prior).

ONSITE AND INTERVIEW SCHEDULING Assero Security consultants and the customer POC will determine the best time and duration for onsite data gathering and interviews. It is usually best to perform the interviews during the onsite data gathering but interviews or follow up interviews can be conducted over the phone.

- The Assero Security consultant will identify the typically roles required to be interviewed and the topics to be covered.
- The customer POC will be responsible for providing the names of those to be interviewed and coordinating the interview schedule.
- The customer POC will be responsible for obtaining necessary permissions, notifications, and physical access necessary.

Data Gathering

- Documentation Review
- Interview Key Stakeholders
- Inspect Controls
- Make Observations
- Conduct Limited External Security Tests

DOCUMENTATION REVIEW

Assero Security consultants will review customer provided documentation (e.g., policies, procedures, audit reports) to collect relevant data on impemented controls. Policies and procedures will be reviewed for:

- Content – completeness of document
- Correctness – correctness of control specifications
- Consistency – consistency within controls between documentest

INTERVIEW KEY STAKEHOLDERS

Assero Security consultants will interview selected key staff members to determine the following:

- Knowledge of their role and responsibility
- Perceived hinderances with performing job functions
- Information regarding recent security incidents or known vulnerabilities
- Understanding of implemented administrative, physical and technical controls and configurations
- Perceived effectiveness of deployed controls

INSPECT CONFIGURATIONS

Assero Security will direct the POC (or delegate) to demonstrate the current security controls ilmplemented on a sample of the servers, workstations, and laptops to gather information regarding the secure configuration of systems.

PERFORM OBSERVATIONS

During the onsite portion of the data gathering process, Assero Security consultants will observe behavior relevant to security controls in scope. These observations will provide additional data reguarding compliance with the customer policies and procedures. Observation may include, but is not limited to the following controls or situations:

- Sensitive information in public areas or waste bins
- Sensitive information discussions in public areas
- Insecure doors to sensitive areas such as data centers or communications closets
- Recorded passwords at workstations
- Visitor control and escort procedures
- Rogue wireless access points

CONDUCT LLIMITED EXTERNAL SECURITY TESTS

The external security testing will examine security controls from external point of view. This test will identify weak passwords, weakness in encryption, and system vulnerabilities that may lead to unauthorized network access, unauthorized information access, or DOS conditions.

Information Gathering. Assero Security will gather data on the customer environment from an extenal point of view using public information and by targeting the subrange of IP addresses provided to Assero Security. This activity will result in device discovery.

Vulnerability Discovery. Assero Security will use a suite of commercial and open source tools to analyze the security controls and scan the external devices for vulnerabilities.

Confirmation and Manual Testing. For each of the identified vulnerabilities, Assero

Security will review, validate, and eliminate any false positives.

Data Analysis

- Document Security Findings
- Determine Potential Remediation Strategies

Document Security Findings

Assero Security consultants will document findings of weaknesses in the current security posture or existing based on the review of the data gathered on each control through the RIIOT (Review, Inspect, Interview, Observe, Test) method.

Determine Potential Remediation Strategies

Assero Security consultants will identify potential security controls and improvements to existing controls to remediate the identified high risk gaps.

3 Deliverables

The following outlines the deliverables regarding this statement of work to be considered complete.

Create Final Information Security Review Deliverables

The following project deliverables will be finalized and provided to the customer:

- **Final Report** – MS Word document containing the following sections:
  - Executive Summary – executve level overview of the project methodology, findings and recommendations
  - Detailed Findings –Report documenting the details of the security program review. This section includes tables and charts of the identified gaps and remediation strategies.

4 Project Scoping Parameters

The following parameters provide a scoping of the service. If significant differences are determined between the actual scope of the service and the parameters below, Assero Security shall negotiate required changes with the customer.

Parameter	Value	Notes
Physical Locations	1	Cleburne County Courthouse
Existing Policies and Procedures	Less than 100 pages	
Key Staff Interviews	3-5 individuals	• IT Director • System Administrator • Customer representative that can speak on sensitive information within the following departments o Personnel o Purchasing o Treasurer o Health & Medical o Tax Office
Systems	Up to 8	To be determined by customer. May include the following: • AS400 • Active Directory • Outlook • Workstations (Windows 7) • Palo Alto Firewalls • WAPs (1 location) • Up to 2 other systems to be determined
Externally Visible IP Addresses	Less than 50	Assero Security will scan up to a class C network with an expectation of less than 50 externally visible IPs answering.
Internal Systems	Sampling	• 2 VLANs • 1 firewalls • 1 database • 2 servers • 2 workstations

4 Project Scoping Parameters

The following parameters provide a scoping of the service. If significant differences are determined between the actual scope of the service and the parameters below, Assero Security shall negotiate required changes with the customer.

Parameter	Value	Notes
Physical Locations	1	Cleburne County Courthouse
Existing Policies and Procedures	Less than 100 pages	
Key Staff Interviews	3-5 individuals	• IT Director • System Administrator • Customer representative that can speak on sensitive information within the following departments o Personnel o Purchasing o Treasurer o Health & Medical o Tax Office
Systems	Up to 8	To be determined by customer. May include the following: • AS400 • Active Directory • Outlook • Workstations (Windows 7) • Palo Alto Firewalls • WAPs (1 location) • Up to 2 other systems to be determined
Externally Visible IP Addresses	Less than 50	Assero Security will scan up to a class C network with an expectation of less than 50 externally visible IPs answering.
Internal Systems	Sampling	• 2 VLANs • 1 firewalls • 1 database • 2 servers • 2 workstations

1) Assumptions

a) Assero

i) Confidentiality. Assero consultants will consider all properly identified information and documentation as sensitive and will handle appropriately.

ii) Notification of Project Delays. Assero project managers will notify the customer project manager of any delays in the project as soon as possible so that project impacts may be discussed quickly.

iii) Limited SOW. Assero is not responsible for performing any services or tasks not specifically stated in this SOW.

iv) Responsibility. Assero assumes no responsibility for other contractors or third parties engaged on related projects to the customer.

b) Johnson County

i) Point of Contact. The customer will provide a single point of contact to assist with the coordination of access to required information, documents, and interviews.

ii) Timely Documents. The customer will provide documents revealing existing policies, procedures, and architecture specifications in a timely manner.

iii) Working Environment. When onsite the customer will provide a safe working environment including workspace, computer monitor, telephone, and network or internet access if required.

iv) Building Access. The customer will provide necessary building, parking and sensitive area access / badges to Assero consultants.

v) Participation. Assero will rely on the customer staff to complete appropriate tasks and participate in interviews. Inability to participate in interviews and complete tasks in a timely manner will affect the completion of the Assero deliverables.

vi) Deliverables Review. Deliverables will be reviewed by the customer and returned to Assero within 5 working days. Acceptance of the deliverable will be assumed if no comments are received from the customer during that time.

2) Change management process

In the event that unforeseen factors change this Services scope of work and/or impact the term and cost of Assero Security-provided Services, Johnson County and Assero Security may mutually revise the SOW and Assero Security shall provide customer with an estimate of the impact of such revisions on the fees, payment terms, completion schedule and other applicable provisions of the SOW. If the parties mutually agree to such changes, a written description of the agreed change ("Change Authorization") shall be prepared, incorporating such changes to the SOW and shall be signed by both parties. The terms of a Change Authorization Form prevail over those of the SOW. A copy of the Change Authorization Form is attached to this Statement of Work.

3) Engagement Related Expenses

Travel and expenses are not included in the estimate and will be billed as incurred. Assero Security will make every attempt to incur reasonable expenses associated with the implementation of the project. Valid expenses typically include parking, meals (unless a per diem is agreed upon), lodging, photocopying and communication costs. Travel costs include: airfare, mileage (if a personal car is used) and automobile rental.

4) Acceptance and Authorization

	Johnson County		October 21, 2013
	Dan Milam		Same as Billing
	(817) 556-6979		
	dmilam@johnsoncountytx.org		

Method: Bi-Weekly [ ] Milestone [ ] At Project Completion [X] Prepaid [ ]

- Assero Security will invoice Johnson County for services performed on a time and materials basis bi-weekly.
- Each invoice is due and payable within 15 days of invoice date

All work will be performed subject to the full terms and conditions listed in the Appendix.

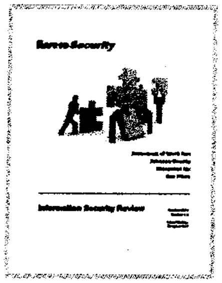
- This offer is valid for 90 days from the date stated above.
- In addition to fees, Assero Security will invoice for, and Johnson County agrees to pay, all reasonable travel and living expenses incurred by Assero Security personnel during the delivery of these services. (No travel is expected for this engagement).

Information Security Review ▪ Project Initiation ▪ Data Gathering ▪ Data Analysis	$3,800.00
Limited External Security Testing ▪ Information Gathering ▪ Vulnerability Discovery ▪ Confirmation and Manual Testing	$1,500.00
Total	$5,300.00

5) Signature

The Statement of Work (SOW) is only valid if signed within 90 days from (Oct. 21, 2013).

By:	By: Doug Landoll Doug Landoll (Oct 21, 2013)
Printed Name: Roger Harmon	Printed Name: Doug Landoll
Title: Johnson County Judge	Title: CEO
Date: 10-28-13	Date: Oct 21, 2013



Johnson County SOW

EchoSign Document History October 21, 2013

Created:	October 21, 2013
By:	Doug Landoll (dlandoll@asserosecurity.com)
Status:	SIGNED
Transaction ID:	XXR2I8BVB3V442U

"Johnson County SOW" History

Document created by Doug Landoll (dlandoll@asserosecurity.com)
October 21, 2013 - 1:34 PM PDT - IP address: 50.84.161.50

Document emailed to Doug Landoll (landolld@gmail.com) for signature
October 21, 2013 - 1:34 PM PDT

Document viewed by Doug Landoll (landolld@gmail.com)
October 21, 2013 - 1:35 PM PDT - IP address: 50.84.161.50

Document esigned by Doug Landoll (landolld@gmail.com)
Signature Date: October 21, 2013 - 1:36 PM PDT - Time Source: server - IP address: 50.84.161.50

Signed document emailed to Doug Landoll (dlandoll@asserosecurity.com) and Doug Landoll (landolld@gmail.com)
October 21, 2013 - 1:36 PM PDT