10-4136-211

SECUVANT
Cyber Security | Risk Management

SECURITY GAP & RISK ANALYSIS

Statement of Work

Presented to:

TOOELE COUNTY

Prepared by:

Secuvant Security Services

Submitted on:

September 19, 2017

Proposal ID: **GRA-RL20170918**
Version: **1A**

REQ. # 137584
P.O. # 138484
VEND # 115714

This STATEMENT OF WORK ("the Agreement") with an effective date of October 1, 2017 (the "Effective Date"), issued pursuant to the terms and conditions included herein, is by and between **Secuvant Security Services** ("Secuvant") and **Tooele County** ("Client"). Capitalized terms not defined herein shall have the same meaning stated in the Agreement.

A. CLIENT CONTACT INFORMATION

Tooele County	**Contact:**	Denise Lawrence
47 S. Main Street, Rm #125	**Phone:**	(435) 843-3202
Tooele, UT 84074	**Email:**	dlawrence@tooeleco.org
Secuvant Security Services	**Contact:**	Ryan Layton
222 S. Main Street # 500	**Phone:**	(801) 390-0601
Salt Lake City, UT 84101	**Email:**	rlayton@secuvant.com

B. STATEMENT OF WORK

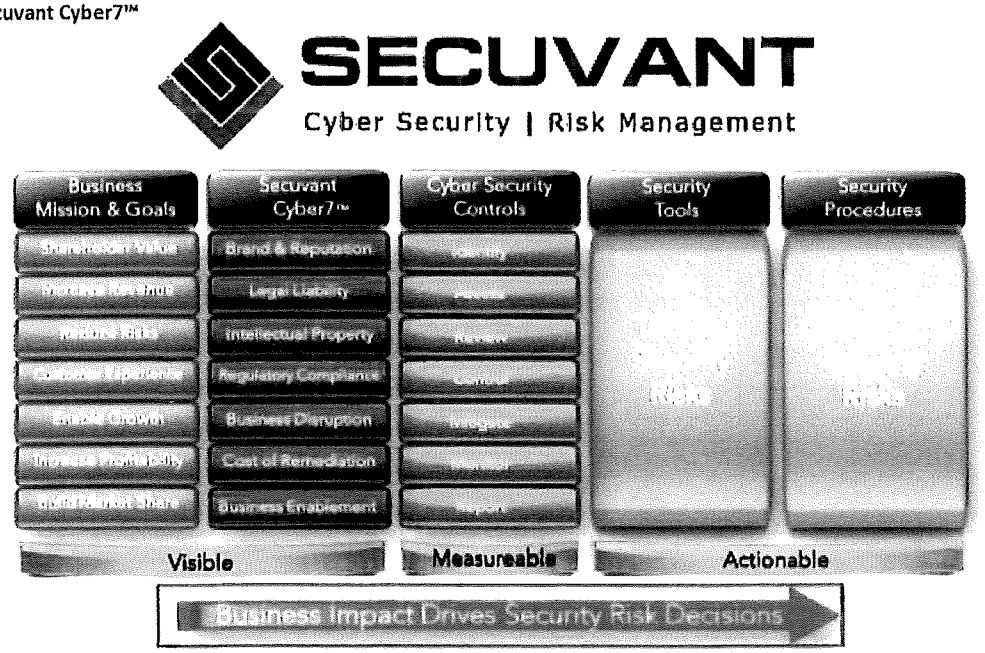
1. EXECUTIVE SUMMARY

Secuvant is pleased to present Client with this Statement of Work for a Security Gap & Risk Analysis. This engagement will include a review of Client's current business landscape; identification and prioritization of business risk using an executive workshop format; assessment of IT security infrastructure, processes, and policies using the ISO-27001 security framework; internal and external vulnerability scanning; internal end-point sensitive data discovery scanning; Microsoft configuration audit scans; review of Client provided documentation; and interviews of key business and technology stakeholders.

Secuvant uses its proprietary Secuvant Cyber7™ methodology (**Figure A**) to identify and align cybersecurity risks with a company's business risks. Priorities of *Brand Protection* and *Legal Liability* will drive differing cybersecurity strategies than that of *Business Disruption* and *Regulatory Compliance*.

Once business risk alignment is accomplished with Client leadership, Secuvant will create a security maturity score for Client based on: a) the ISO-27001 standard, b) business risk alignment findings, and c) output from technical scans. This security maturity score provides Client with enhanced visibility to prioritize risk areas needing immediate attention, realign security investments to current business priorities, and create resource and funding strategies.

Figure A: Secuvant Cyber7™



2. SCOPE OF SERVICES

Secuvant will perform a Security Gap & Risk Analysis for Client. The assessment includes:

a. Qualitative analysis. Qualitative data is obtained via an Executive workshop with Client's senior leadership team (see appendix), and continues with ongoing workshop sessions with core team members as required.

b. Quantitative analysis. Quantitative data is obtained via discovery and analysis of three scan types:
   i. **Sensitive Data Discovery Scan**. Scope includes scans up to 100 end-points. The scan of in-scope devices will identify where sensitive information that is vulnerable to theft and misuse (credit card numbers, social security numbers, and Driver's License numbers) is stored in Client's end-point environment.
   ii. **Microsoft Configuration Audit Scans**. Scope includes scanning and security audit of all Windows server configurations in Client environment.
   iii. **Internal and External Network Vulnerability Scans**. Scope includes scanning of up to 512 IP addresses per vulnerability scan. Additional scans of up to 512 IP addresses will be performed until Client's specified scope has been scanned.

All scoping for the Quantitative analysis shall be documented in a Vulnerability Scanning Authorization and Scoping Document, a spreadsheet provided by Secuvant to Client. All devices scanned are collectively

referred to as "In-scope Devices". Secuvant will perform the three technical scans using a combination of both third-party and proprietary scanning software.

Upon completion of the scans, a Secuvant Consultant(s) will analyze the output of the scans, workshops, and interviews, and will provide a deliverable detailing the potential IT and other business risks associated with the people, processes, and technologies utilized within Client's business operation. Furthermore, Secuvant will use this information to create a detailed project plan for immediate execution towards security program maturity.

3. DELIVERABLES

Deliverables included with this SOW are as follows:

- Cyber Security Business Impact Analysis and Business Alignment Summary
- Technical Security Scans: Summary and Detail Reporting
- Gap Analysis Findings and Maturity Modeling Report
- Cyber Risk Program Management Planning Document (Security Maturity Roadmap)

4. PERSONNEL

Secuvant will provide security professionals to perform the required roles to execute this SOW. Client acknowledges and agrees that Secuvant may retain the services of subcontractors to perform or assist Secuvant in performing services under this SOW. All subcontractors shall be independent contractors and will perform services under Secuvant's direction and control.

5. TIME-LINE

Secuvant estimates project completion to be achieved in approximately four (4) to six (6) weeks based on the Scope, Approach, Deliverables, Personnel and the Responsibilities stated herein. If the Project is delayed for any reason outside of Secuvant's direct control, Secuvant may issue a Change Order per the Change Order Process stated herein, which may necessitate additional time and/or Fees.

6. RESPONSIBILITIES

Secuvant will agree to the following obligations under this SOW:

- Consider Client information as confidential and handle all documentation and information provided to it pursuant to the terms of non-disclosure agreement and/or the Agreement, as applicable.
- Identify when any subject-specific knowledge is necessary from Client and notify Client's Project Sponsor that such information is required.

- Notify Client of any known Project risks or situations that may adversely impact the Project in order to determine ways to manage such impact that could include changes to Timeline, Scope or Fee.

Client will perform the following obligations under this SOW:

- Provide access to in-scope devices
- Provide a list of departments located in the in-scope facilities to be assessed.
- Provide a list of internal and external IP addresses for in-scope devices to be scanned.
- Assign Client personnel, including executives as required for the Executive Workshop, to (a) perform required technical tasks, (b) attend workshops and participate in good faith, (c) Assist Secuvant (as needed) to create the Deliverables as stated in the Deliverables section, including a full 8-hour day for a workshop to answer questions related to the analysis.
- Provide on-site workspace, phone, and Internet access for Secuvant personnel as required at no additional cost to Secuvant.
- Review the interim, draft, versions of the Deliverables prior to their formal submission by Secuvant. State its final acceptance of the Deliverables within five (5) business days of Deliverable submission. If final acceptance is not stated within such period, it will be deemed given.

7. EXCLUSIONS

- Secuvant will not be providing software or hardware tools, or associated licenses, to become the property of Client after the engagement.
- Secuvant does not provide any guarantee that if the recommendations are followed Client will be free of risk or loss. Secuvant will not be responsible for any past, present or future incident, breach or loss.
- Remediation efforts for any of the recommendations are not included in this scope. Any active remediation, patching, or changes may be provided in the future at additional costs. This SOW is for analysis and reporting only.

8. CHANGE ORDER PROCESS

If the scope of the services or any material item herein is changed or needs to be changed, one party will prepare and submit to the other the Change Order. Client acknowledges that any material change, including but not limited to a change in the Objectives, Scope, Timeline, etc. will result in a Change Order that may necessitate additional Fees. The recipient of a proposed Change Order shall have two (2) business days to review the proposed Change Order. Only a counter-signed Change Order will modify the obligations stated herein.

9. PROFESSIONAL SERVICE FEES

Service Offering	Description	Total Price
PS-GAP-ANALYSIS	Secuvant Security Gap & Risk Analysis	$17,500
PS-EXPENSES	Customary Travel and Expenses	N/A
Total Amount Due	Total Price to Perform Services	**$17,500**

Payment Terms: **50% due upon acceptance** of proposed SOW, with the remaining balance due at completion of services to be performed. Late payments are subject to a late fee of 1.25% per month beginning 15 days after payment due date.

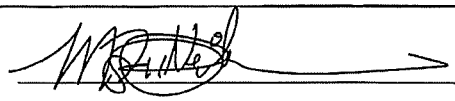
Secuvant's submittal of this SOW is its proposal to Client to perform the services for the Fee stated herein. The proposal is valid for thirty (30) calendar days from the date on the cover page of this SOW. If Client does not cause a duly authorized representative to affix his/her signature to this proposal within such period, this proposal is retracted and becomes null and void. Client, by causing a duly authorized representative to affix his/her signature below, is making an offer to Secuvant to enter into an agreement pursuant to the terms stated herein. If Secuvant counter-signs this SOW, but services do not commence within ninety (90) business or calendar days after the date of Client's representative's signature, Secuvant may terminate this SOW with no further obligation to Client.

C. ACCEPTANCE

ACCEPTANCE: In witness whereof, the parties hereto have caused this Statement of Work to be executed by their duly authorized representatives as of the Effective Date, and this Statement of Work, attached Exhibits and Appendices and its accompanying terms and conditions set forth below shall become a legally binding agreement upon the execution of both parties.

Agreed to and accepted by: Wade B Bitner 6 DECEMBER 2017

Secuvant Security Services **Client**

By:		By:	Wade B Bitner
Name:	Todd Neilson	Name:	WADE B. BITNER
Title:	COO	Title:	COMMISSION CHAIRMAN
Date:	December 11, 2017	Date:	6 DECEMBER 2017

D. TERMS AND CONDITIONS

1. CONFIDENTIALITY: Secuvant will safeguard information directly obtained from scanning the devices, to the extent reasonably understood to be confidential, from unauthorized disclosure using no less than the same care Secuvant affords its own confidential information of a like information. Secuvant will not use such information for any purpose other than in connection with performing and evaluating the services described herein. Secuvant's obligation to keep information confidential does not apply to information that (i) is or becomes generally available to the public other than as a result of a disclosure by Secuvant; (ii) is obtained outside of this agreement and is in Secuvant's rightful possession without an obligation of confidentiality; or (iii) is required to be disclosed by operation of law.

2. LIMITATION OF LIABILITY: In no event will Secuvant be liable for any direct, indirect, special, incidental, or consequential damages arising out of, or in any way connected with, this agreement or the products and services described herein, including, without limitation, lost business or lost profits, whether foreseeable or not, even if the other party has been advised of the possibility of such damages. Secuvant does not warrant that the services will detect every vulnerability in your environment, or that Secuvant's security assessments, suggested solutions, or advice will be error-free or complete. You agree that Secuvant will not be responsible or liable for the accuracy or usefulness of any information provided by Secuvant, or for any use of such information. Secuvant provides its services on an "as is" basis. Secuvant disclaims any and all warranties, express or implied, including without limitation warranties of merchantability and fitness for a particular purpose, with respect to its services. Secuvant does not warrant or covenant that the services or deliverables or any results, report, recommendations, judgment, assessments, opinions, or conclusions will be error free or comprehensive, but they are provided in good faith. Client is solely responsible for acting on any results, report, judgment, assessments, opinions, or conclusions provided by Secuvant.

3. In no event will either party be liable for any consequential, incidental, indirect, cover, exemplary, special, or punitive damages or for any loss of profits, revenue or business, even if advised of the possibility thereof. In no event will a party's aggregate liability for any and all claims and causes of action under this agreement or relating to its subject matter exceed the total amount paid to Secuvant under this agreement. Further, Secuvant does not warrant, promise or guarantee specific outcome regarding safety from data breach or other adverse information security, integrity or availability events. No information security program can eliminate all risk of data breach or system compromise. Secuvant further does not guarantee any specific outcome regarding any SSAE 16 or service organization controls review of any type conducted by a third party. Client acknowledges and agrees the foregoing disclaimer and holds Secuvant harmless in the event client suffers a data breach or other adverse information security event, absent a showing of bad faith, willful misconduct, or gross negligence by Secuvant or its agents. This section does not apply to or excuse client from any obligation to pay fees or reimburse expenses.

4. INDEMNIFICATION: Client hereby agrees to indemnify and hold harmless Secuvant, its employees, agents, representatives, directors, officers, and shareholders, from and against any and all liabilities, claims, damages, causes of actions, losses, expenses and judgments (including attorney's fees) arising out of, or in connection with, the services to be provided under this Agreement.

5. TERM AND TERMINATION: Secuvant shall serve as a consultant to the Client for the period listed in the body of the SOW. Notwithstanding the foregoing, either party may terminate the SOW for material breach of the other party if such breach remains uncured for seven (7) days after written notice to the other party. In the event of such termination, Secuvant shall be paid for the pro-rata portion of the services that have been performed in accordance with this SOW prior to notice of termination. Confidentiality provision and Intellectual Property Rights provision, Indemnification provision, Limitation of Liability provision, Relationship of Parties provision, Governing Law provision, and Entire Agreement provisions shall survive termination of this Agreement.

6. OWNERSHIP OF DELIVERABLES: For purposes of this Agreement, Deliverables shall mean all work product first created by Secuvant for delivery to Client in connection with the Services provided hereunder. Client shall be the owner of the Deliverables. Notwithstanding the foregoing, Secuvant shall be the owner of all Secuvant's Confidential Information, images and graphics, trademarks, and all visual models, graphs, and other graphical representations contained in any Deliverable and any work product first created by Secuvant in any manner, whether in connection with the Services provided hereunder, or otherwise.

7. COMPLIANCE WITH LAWS: Each party shall, in its performance hereunder, comply with all applicable laws and regulations (including, without limitation, laws concerning bribery, corruption and prohibited business practices).

8. FORCE MAJEURE: In no event shall Secuvant be responsible or liable for any failure or delay in the performance of its obligations hereunder arising out of or caused by, directly or indirectly, forces beyond its control, including, without limitation, accidents, acts of war or terrorism, civil or military disturbances, nuclear or natural catastrophes or acts of God, and interruptions, loss or malfunctions of utilities, communications or computer (software or hardware) services; it being understood that the Trustee shall use reasonable efforts which are consistent with accepted practices in the banking industry to resume performance as soon as practicable under the circumstances.

9. RELATIONSHIP OF PARTIES: Secuvant is a non-exclusive, independent contractor, and nothing in this SOW or done pursuant to this SOW will create or be construed to create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

10. GOVERNING LAW: The validity, interpretation, construction and performance of this SOW shall be governed by the local, state and federal laws of the State of Utah and the United States, without giving effect to the principles of conflict of laws.

11. CHOICE OF VENUE: Any action or proceeding seeking to enforce any provision of or based on any right arising out of this Agreement may be brought against the Secuvant or Client only in the courts of the State of Utah or, if it has or can acquire jurisdiction, in the United States District Court for the District of Utah, and Secuvant and Client consent to the jurisdiction of such courts (and of the appropriate appellate courts) in any such action or proceeding and waives any objection to venue laid therein.

12. ENTIRE AGREEMENT: This SOW, including all attachments, constitutes the entire agreement between the parties as to its subject matter and supersedes all previous and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject matter. Except as set forth herein, no modification, amendment, or waiver of any provision of this SOW will be effective unless in writing signed by both parties. Notwithstanding any language to the contrary therein, no terms or conditions stated in any Secuvant purchase order or Client remittance will be incorporated into or form any part of this Agreement, and all such terms or conditions will be null and void.

13. EXCLUSION OF ADDITIONAL TERMS: Secuvant and Client agree that any terms and conditions on a purchase order, check, or other financial instrument issued to pay the Fee, or a portion thereof, as defined herein, shall be of no force or effect and that the purchase order, check, or payment instrument will be effective only with regards to payment, not to add to or revise any provisions herein or of the Agreement.

APPENDIX A: WORKSHOP AGENDA

TIME	*TOPIC*	*TEAM*
Session 1: Business Risk / Prioritization Workshop – Executive Team		
8:30 - 10:00 AM	**Executive Team Business / Security Alignment** • Business baseline discussion • Business prioritization discussion o Revenue Streams o Critical business processes o Secuvant Cyber7™ • Business impact areas due to failed security **NOTE: See page three (3) for Executive Workshop discussion outline.**	• IT Leadership Team • Chief Financial Officer • Chief Operating Officer • Chief Executive Officer • Chief Risk Officer • VP of Operations • VP of HR • VP of Marketing • Others by invitation
Session 2: Security Framework Workshop – Core Assessment Team		
10:00 - 10:30 AM	**Technical Kick-off Meeting** • Meeting overview, scope & objectives • Validate 's goals & objectives • Structural overview, e.g. operating companies, divisions, locations, departments • Operating organizational overview, e.g. IT organization(s), major functional areas, reporting relationships, etc. • Current systems overview, e.g. major app systems diagrams, high-level data center schematics, network & connectivity schematics, etc. Your security vision – Top level security strategy & issues overview • Get Credentials, IP Addresses, end-points, scope, etc. for scanning activities	• Chief Security Officer • Key Functional Execs • Business Area Owners • IT Director • Architecture Team • Audit & Compliance
10:30 – 12:00 PM	**ISO 27001/17799 Question Mapping** • Risk Management • Security Policy • Organization of Information Security • Asset Management • Human Resources • Physical and Environmental • Communications and Operations Management • Access Control • Information Systems Acquisition, Development and Maintenance • Information Security Incident Management • Business Continuity Management • Compliance	• Core Team • Chief Security Officer • Regulatory & Compliance • Internal Audit • Sr. Architect • Development Director • IT Director • Security Director
12:00 - 1:00 PM	**Lunch Break**	• All

1:00 - 3:00 PM	**Security Environmental Domain Questions** • Security Architecture and Models • Security Management Practices • Access Control Systems and Methods • Telecommunications and Network • Operations • Cryptography • Application and System Development • Physical Security • Disaster Recover and BCP • Compliance and Governance • Database Security	• Core Team • IT Director • Systems Director • Network Director • Telecom Manager • Physical Security Manager • Compliance Officer • DBA Manager
3:00 - 4:00 PM	**Wrap Up and Next Steps** • Time-lines • Expected deliverable deadlines	• Core Team • CIO/VP of IT • IT Director • Business Owner/Lead

Time Commitments:

- *Core assessment team.* Those leading the assessment. Typically, someone from the security/risk management team, executive team and application team. These people are required for the full day since they should be in all of the sessions. We've had times when someone had to step out for a critical meeting, but for the most part those people are giving up their time for the entire engagement. **[Full Day]**

- *Regulatory Compliance team*: Internal Audit, key business owners (e.g.: HR, Finance), data architect. **[1 hour]**

- *Security/Risk Management team*: IT security, Network Team, Enterprise Architect/Data Architect. **[2 hours]**

- *Custom Application Development*: development manager, lead developer, application owners. **[30 minutes]**

- *Business Applications administrators/owners*: These are the people that administer/own things like ERP systems (egg: SAP, eBusiness, Peoplesoft, Financials, HR). **[30 minutes]**

- *Database Administrators*: DBA team including lead DBA, DBA manager, etc. **[1 hour]**

- *Storage & System Administrator team*: Server administrators, Storage Admins (if different from server admins). **[30 minutes]**

- *Networking*: Someone who understands how 's network is put together including how security tools like firewalls, SIEM, NAC, etc. are deployed and used. **[30 minutes]**

APPENDIX B: EXECUTIVE WORKSHOP DISCUSSION OUTLINE

NOTE: This is a NON-TECHNICAL workshop designed for Executives. The workshop facilitates discussion within the Executive Team around the organization's business objectives and known business risks. The desired outcome of the workshop is consensus on prioritization and alignment of Cyber Risk to the business.

BUSINESS BASELINE DISCUSSION

- Corporate Culture – Corporate mission and goal review, employee sentiment toward cyber risk, etc.
- Management Systems – Visibility and systems that manage the business
- Operational Systems – Processes and procedures related to risk
- Resource Management – Current and Future
- Products and Services – Revenue streams, Lines of business, and their associated risks
- Customers & Markets – focus areas, governance, compliance and growth plans
- Business Foundations – Market entry, exits and risk processes and procedures

COMPANY PRIORITIES – SECUVANT CYBER 7™ RISK AREAS (Determines Security plan recommendations)

- Brand and Reputation – Risks of damage, control, press, corporate value, integrity, mitigation
- Compliance and Governance – Areas of audit, PCI, PII, PHI, HIPAA, etc.
- Intellectual Property Protections – Confidentiality and data security of IP, controls, areas of concern
- Business Disruption – Availability and uptime, product management, efficiencies
- Costs of Breach Remediation – Awareness, Notifications, loss of business, uptime, Isolation, Disaster recovery and business continuance
- Legal Liability – Cyber Liability insurance, risk assignment and acceptance
- Business Enablement – Using cybersecurity to protect existing revenue, capture new revenue

BUSINESS ENABLEMENT

- Operational – Internal controls, policies, SOD, staffing, change control
- Strategic – Financial controls, needs, changes, improvements to risk management
- Technology – Integrity of systems, priority of systems that support business, dependencies, integration strategy
- Human Resources – Awareness, training, testing, policy, governance
- Tactical – Network access controls, Lock down vs. Enablement, Supply Chain