



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at wvOASIS.gov. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at WVPurchasing.gov with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 2

List View

General Information

[Contact](#) | [Default Values](#) | [Discount](#) | [Document Information](#)

Procurement Folder: 605438

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0803

Vendor ID: VS0000019687

SO Doc ID: DOT2000000022

Legal Name: IBM Corporation

Published Date: 8/14/19

Alias/DBA:

Close Date: 8/29/19

Total Bid: \$0.00

Close Time: 13:30

Response Date: 08/29/2019

Status: Closed

Response Time: 12:51

Solicitation Description: EQUIP LEASE/RENTAL WITHOUT OPERATOR 6620C009

Total of Header Attachments: 2

Total of All Attachments: 2



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 605438

Solicitation Description : EQUIP LEASE/RENTAL WITHOUT OPERATOR 6620C009

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-08-29 13:30:00	SR 0803 ESR08291900000001308	1

VENDOR

VS0000019687

IBM Corporation

Solicitation Number: CRFQ 0803 DOT2000000022

Total Bid : \$0.00 Response Date: 2019-08-29 Response Time: 12:51:16

Comments: We were unable to respond to solicitation CRFP : ISC2000000001 so we are responding here

FOR INFORMATION CONTACT THE BUYER

Crystal G Hustead
(304) 558-2402
crystal.g.hustead@wv.gov

Signature on File

FEIN #

DATE

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	EQUIPMENT LEASE/RENTAL WITHOUT OPERATOR	0.00000	EA	\$1,376,600.000000	\$0.00

Comm Code	Manufacturer	Specification	Model #
72141702			

Extended Description :	EQUIPMENT LEASE/RENTAL WITHOUT OPERATOR PER EXHIBIT A PRICING PAGE AND INFORMATION ATTACHMENT FORM
-------------------------------	--

Comments: We were unable to respond to solicitation CRFP : ISC200000001 so we are responding here

1. Cost Sheet

Item	Description	Unit Cost	Unit of Measure	Estimated Quantity	Extended Cost
1	Cyber Security Risk Program		LS	1	\$1,091,600.00
2	Post Implementation Hourly Consultant Rate		HR	1,000.00	\$285,000.00
Total Bid Amount					\$1,376,600.00

Phase		Typical Outcomes / Program Deliverables	Mapping to RFP Milestones	Price
1	Project Initiation and Program Planning	<ul style="list-style-type: none"> Kick Off Presentation Workshop Agenda Stakeholder listing 	<i>A.2.2.3 Program Roadmap</i>	\$149,100.00
2A	Program Design and Framework Development	<ul style="list-style-type: none"> Cyber Risk program charter (including: key goals and objectives, executive owners and sponsors, program scope and applicability, intended audience, target program schedule with milestones) Target operating model (TOM) / Enterprise interaction model across three lines of defense Critical information asset inventory with business hierarchy (contextual data / metadata) Department and Agency level inherent Risk Profile classification model (tiered model) and procedure Completion of Risk Profiling – pilot set 	<i>A.2.2.1 Development Information Security Framework</i>	\$178,400.00
2B	Program Documentation, Pilot, and Finalization	<ul style="list-style-type: none"> Draft Cyber Risk Framework Cyber Security / IT Risk policies and standards Standard operating procedures (if applicable) Risk reporting templates Program roadmap Roles and Responsibilities (RACI) between central teams and agencies Documented approach for agencies to apply framework Risk Assessment Results for pilot set of “systems” (applications or infrastructure) – with one small agency and one large agency Updated Cyber Risk Framework document(s) 	<i>A.2.2.2 Reporting Templates</i> <i>A.2.2.8 Assessment Results (for pilot set only)</i>	\$538,800.00

Phase		Typical Outcomes / Program Deliverables	Mapping to RFP Milestones	Price
3	Two (2) Vendor Solicitations: <ul style="list-style-type: none"> • 3A – Assessment Vendor • 3B – GRC Vendor 	<ul style="list-style-type: none"> • Two Solicitation documents 	<i>A.2.2.4 Third-party procurement solicitations quantity two (2)</i>	\$103,200.00
4	Vendor Selection*** & GRC Tool Technical Implementation by GRC Vendor***	<ul style="list-style-type: none"> • Out of scope for IBM 	<i>A.2.2.5 Implementation of governance tool – *** dependency on WVOT, GRC Vendor, and selected GRC Tool</i>	\$0
5	Program Rollout Planning	<ul style="list-style-type: none"> • Program roll-out plan • High level training sessions for users on use of the governance tool (up to two 1-hour sessions) 	<i>A.2.2.6 Agency roll-out plan</i>	\$57,500.00
6	Program Operating Model Support	<ul style="list-style-type: none"> • Operational Model for Cyber Risk Program based on a charge-back model 	<i>A.2.2.7 Policies and operations procedures</i>	\$64,600.00
7	Governance and PMO	<ul style="list-style-type: none"> • Communication plan • Periodic Project Status meetings (e.g. monthly, biweekly, etc. as needed) • Support contact matrix / escalation matrix (detailing on-site support for major milestones and project initiatives) 		

Disclaimer:

IBM is able to provide additional hourly rates based on the scope of service. IBM will provide hourly rates based on nature of the requirement to be performed for the state.

2. Appendix A

Pursuant to the instructions of this solicitation, International Business Machines Corporation (“IBM” or “Vendor”) offers its clarifications and proposed modifications to the terms and conditions listed in **RFP (OT19152)** (the “RFP”), as set forth below. During negotiations with the State of West Virginia, IBM reserves the right to identify and negotiate terms and conditions in addition to those listed herein. IBM’s proposal is expressly conditioned upon the negotiation of a mutually acceptable set of terms and conditions.

RFP Provision	IBM’s Proposed Alternative Language
<p>36. INDEMNIFICATION:</p> <p>The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.</p>	<p><i>The below provision agreed to between the State of WV and IBM on 2/27/2017.</i></p> <p>INDEMNIFICATION AND LIMITATION OF LIABILITY:</p> <p>Vendor shall defend, indemnify, protect, save and hold harmless, to the extent Vendor is legally liable, Agency, its officers and employees from and against any and all claims or causes of action, damages or costs, including attorney's fees, for patent, copyright, trademark or trade secret infringement, and bodily injury or damage to real or tangible personal property, arising from the negligent or willful acts or omission of the Vendor, or its agents, employees, or subcontracts in the performance of this Contract. Vendor shall not be liable for damage that are the result of negligence or intentional wrong doing by the Agency or its employees. This clause shall not be construed to bar any legal remedies the Vendor may have with Agency's failure to fulfill its obligations pursuant to this Contract.</p> <p>Agency agrees that the Vendor, its principals, members and employees shall not be liable to the Agency, unless otherwise stated in the applicable Addendum, for any actions, damages,</p>

	<p>claims, liabilities, costs, expenses, or losses in any way arising out of or relating to this Contract or the Products provided or Services performed hereunder for an aggregate amount in excess of two times the value of the Products provided or Services performed under this Contract. The foregoing limitation does not apply to patent, copyright, trademark or trade secret infringement claims for which Vendor must indemnify Agency under this Contract, or to damages resulting from bodily injury caused by the Vendor's negligence. In no event shall the Vendor be liable for any indirect, special, punitive, or consequential damages arising out of this Contract or the use of the Products or Services purchased by the Agency hereunder, loss of, or damage to, data, lost profits, business, revenue, goodwill, or anticipated savings even if the Vendor has been advised of the possibility of such damages. Both parties agree that this Contract does not create any right or cause for any third party against the other except for third party claims that fit within the identification provision of this Contract.</p>
<p>The adjacent provision proposed by IBM to be added >>></p>	<p>45. European General Data Protection Regulations.</p> <p>The State and Agency agree that no State or Agency personal data that is subject to European General Data Protection Regulations (GDPR) requirements will be provided to Vendor under this Contract.</p> <p>In the event of a change, the State and Agency will notify Vendor in writing and a Data Processing Addendum (DPA) agreed to between the parties will apply and supplements the Contract</p>



August 29, 2019

Subject: CRFP ISC2000000001 – WVOT RFP for Cyber Risk Program

To Whom It May Concern:

On behalf of IBM, I would like to thank you for the opportunity to respond to the above referenced RFP. We understand the importance of this key initiative to WVOT. Security attacks in this industry are accelerating, and the attack vectors are becoming more diverse with government agencies and associated entities continuing to be a major target. A comprehensive cyber security and risk management program is essential.

Our objective for this proposal is to further demonstrate why we are well qualified by presenting what we believe differentiates IBM from the competition. These include:

Our Experience – We have extensive experience in developing cyber security and risk management programs. We have experience serving multiple US state governments and their agencies on cyber security related topics. We partner with a large number of partners in the security industry to bring the right solutions to our Clients.

Our Engagement Team – We bring dedicated security services professionals at all levels of our team, with many years of combined security experience. Additionally, our team members have extensive experience in conducting security assessments, developing security strategies and roadmaps, developing sustainable and repeatable processes to maintain security in complex organizations, as well as standing up and staffing risk management functions within multi-tiered organizations along the lines of the ISACA three lines of defense model. Many of our engagement team members have held positions in industry.

Our Quality Methodologies Based on Practical Experience – Our approach is based on industry standards and best practices. Our recommendations and work products will be based on recognized rules, policies, and standards to help build strong security and provide support for compliance.

This industry knowledge and expertise is augmented by over 8,000 IBM security professionals engaged worldwide in both consulting and in day to day security services protecting over 12,000 customers worldwide.

We look forward to earning the right to tell you more about our proposal.

Thank you.
Sincerely,

Bradley Bone
Security Services Leader – Eastern US
IBM Security Services
Ph: +1 (321) 505-3066
Email: Brad.Bone@ibm.com

Proposal for

West Virginia Office of Technology (WVOT)

CRFP ISC2000000001
Cyber Risk Program

Table of Contents

Executive Summary	4
Our Understanding of Your Goals	4
Our Proposed Solution Overview	4
Description of Proposal	6
1. IBM’s Point of View (POV)	6
1.1 IBM Methodology	6
1.2 References to Industry Standards.....	7
2. Overall Approach.....	8
2.1 Summary of Proposed Approach	8
2.2 Engagement Outcomes and Key Deliverables	8
2.3 Proposed Engagement Timelines	10
2.4 Team Composition / Delivery Model	11
2.5 Scope Definition and Related Assumptions	12
3. Detailed Statement of Work	12
4. Qualifications and Experience	21
4.1 Representative Client Success Stories	21
4.2 Representative Consultant Profiles.....	22
5. Key Success Factors.....	25

Executive Summary

Our Understanding of Your Goals

We understand that West Virginia Office of Technology (WVOT), Cyber Security Risk Program needs to be turnkey and performance-based, with responsibility for engaging directly with your key enterprise stakeholders and IT service providers that are accountable for managing risks to acceptable levels through remediation or other relevant actions. IBM also understands that IBM is looked upon to provide thought leadership, drive efficiencies on an ongoing basis, and continuously improve the overall risk posture.

To summarize, we understand that your goals from this RFP are as follows:

1. To build and document a formal Cyber Risk Program including core building blocks, associated processes and procedures, and supporting artefacts.
2. To implement the Cyber Security Risk Program based on industry standards with supporting software-based Governance Risk and Compliance (GRC) tools to enable it.
3. To build an operational program that can be methodically rolled out to departments and agencies across the state in a phased and structured manner.
4. To formalize the operating relationships and interactions between the agencies and the centralized cyber risk program office.

Our Proposed Solution Overview

Our response to your requirements focuses on building a robust approach aligned with the needs of your operational and business needs. We are confident that we have provided you with a proposal for building and implementing a turnkey performance-based Cyber Security Risk Program that will protect your departments' and agencies' most critical assets and services.



Description of Cyber
Security Risk Program
Proposal

Description of Proposal

1. IBM's Point of View (POV)

This section provides a high-level overview of IBM Security's point of view on an integrated cyber security risk management program ("Cyber Risk Program").

1.1 IBM Methodology

An integrated cyber risk program is an integral component of an organization's information technology strategy and broader enterprise risk management (ERM) framework. The figure below illustrates IBM's methodology for cyber security *governance, risk, and compliance (GRC) management* – it depicts a lifecycle-based approach to cyber security risk management.

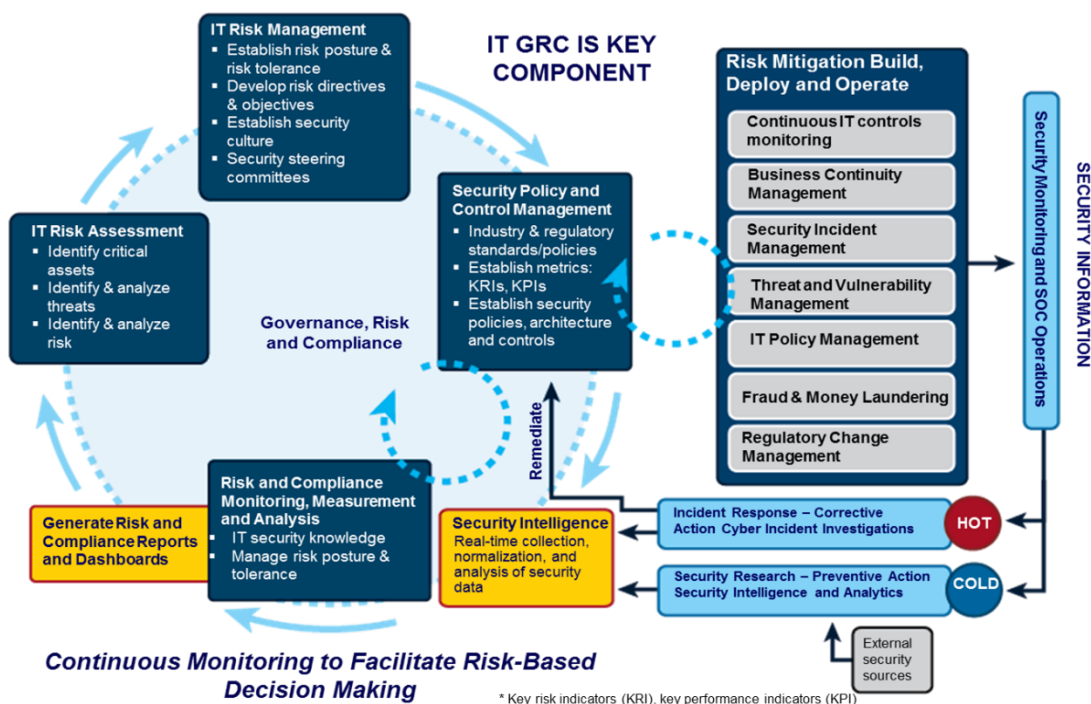


Figure 1: IBM Methodology for GRC Management

Key highlights of IBM's methodology include:

- Lifecycle Based Model for Continuous Improvement* – A “plan-do-check-act” (PDCA) type life cycle model for continuous monitoring, feedback, and improvement of the organization's risk posture and overall security program
- Policy Management* – Ability to define, develop, socialize, implement, and periodically update the information security policies in alignment with business requirements as well as industry standards, legal and regulatory compliance requirements, and best practices.

- iii. *Business Process Mapping* – An ITRM framework that effectively maps key business processes with risks and controls associated with the use of technology to support the delivery of West Virginia Office of Technology (WVOT)’s business objectives
- iv. *Ongoing Assessments* – Ongoing risk and controls assessments (self- or third-party assessments) across various parts of the security program to measure the effectiveness of implemented and/or mitigating controls
- v. *Integrated Security* – Ability to integrate with security operations (SOC), security threat intelligence (cyber lab), network operations, etc. type functions in order to deliver real-time collection, normalization, and analysis of security data and appropriately map them back to IT risks (for e.g., vulnerability management, patch management, configuration management, etc.)
- vi. *Risk Monitoring* – A real-time, current, and accurate IT Risk Register that serves as the authoritative book of record to monitor current IT related risks across the enterprise
- vii. *Prioritized Remediation and Exceptions Management* – Ability to use business context to determine risk and device remediation action plans to address areas of highest risk, and then automatically update the IT Risk Register upon successful completion of remediation efforts
- viii. *Operational Metrics and Key Indicators* – Implementation of real and meaningful metrics, including key performance indicators (KPI) and key risk indicators (KRI) across the process, risk, and controls framework in order to measure the effectiveness of controls
- ix. *Reporting* – Executive Reports and Dashboards for effective visibility and risk-based decision-making in order to appropriately address and manage the areas of highest risk

1.2 References to Industry Standards

IBM’s overall POV as well as our methodology and proposed approach in this document is fully aligned with recommended and best practices outlined in relevant industry standards, such as the following, at a minimum.

No.	Standard / Guideline	Title
1	NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
2	NIST SP 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
3	NIST SP 800-30 Rev. 1	Guide for Conducting Risk Assessments
4	NIST Cyber Security Framework (CSF)	This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
5	NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations
6	ISO/IEC 27000-series	Recommendations on information security management – the management of information risks through information security controls

2. Overall Approach

This section provides a high-level description of IBM’s proposed phased approach to design, build, and roll out WVOT’s Cyber Security Risk Management program (“Cyber Risk Program”), including key phases, engagement deliverables and outcomes, indicative timelines, and any relevant scope assumptions.

2.1 Summary of Proposed Approach

The figure below illustrates our high-level approach with the main phases. First, as can be seen below, our approach breaks down the overall program into key phases with tangible outcomes and deliverables from each phase, and measurable milestones and completion criteria defined for the end of each phase. Second, our approach combines our strong understanding of industry standards (such as the NIST SP 800-series listed above) with our practical experience from having built IT risk management functions within other organizations using a crawl-walk-run type model. Lastly, Section 2.2 below provides a brief mapping of the deliverables from each phase of our approach back to your RFP requirements to help demonstrate the completeness of our approach.

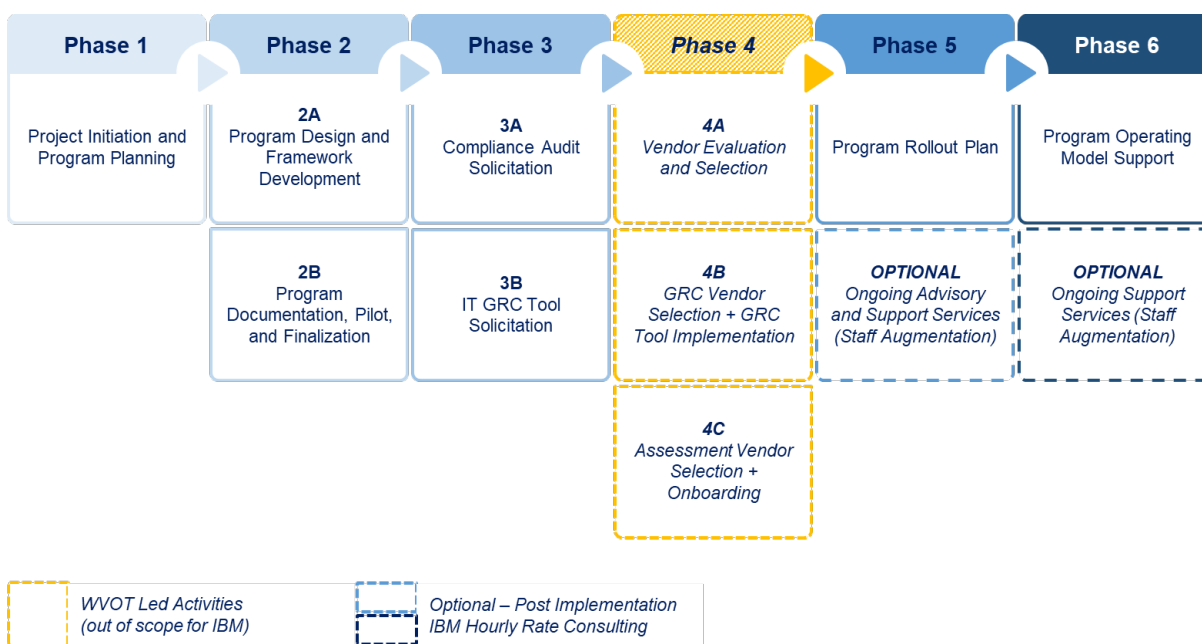


Figure 2: Proposed Approach

2.2 Engagement Outcomes and Key Deliverables

The table below provides a list of the typical outcomes from each Phase of IBM’s proposal. Please refer to Section 3 Detailed Description of Services for a full listing of formal deliverables from each phase and activity.

Phase		Typical Outcomes / Program Deliverables	Mapping to RFP Milestones
1	Project Initiation and Program Planning	<ul style="list-style-type: none"> • Kick Off Presentation • Workshop Agenda • Stakeholder listing 	<i>A.2.2.3 Program Roadmap</i>
2A	Program Design and Framework Development	<ul style="list-style-type: none"> • Cyber Risk program charter (including: key goals and objectives, executive owners and sponsors, program scope and applicability, intended audience, target program schedule with milestones) • Target operating model (TOM) / Enterprise interaction model across three lines of defense • Critical information asset inventory with business hierarchy (contextual data / metadata) • Department and Agency level inherent Risk Profile classification model (tiered model) and procedure • Completion of Risk Profiling – pilot set 	<i>A.2.2.1 Development Information Security Framework</i>
2B	Program Documentation, Pilot, and Finalization	<ul style="list-style-type: none"> • Draft Cyber Risk Framework • Cyber Security / IT Risk policies and standards • Standard operating procedures (if applicable) • Risk reporting templates • Program roadmap • Roles and Responsibilities (RACI) between central teams and agencies • Documented approach for agencies to apply framework • Risk Assessment Results for pilot set of “systems” (applications or infrastructure) – with one small agency and one large agency • Updated Cyber Risk Framework document(s) 	<i>A.2.2.2 Reporting Templates</i> <i>A.2.2.8 Assessment Results (for pilot set only)</i>
3	Two (2) Vendor Solicitations: <ul style="list-style-type: none"> • 3A – Assessment Vendor • 3B – GRC Vendor 	<ul style="list-style-type: none"> • Two Solicitation documents 	<i>A.2.2.4 Third-party procurement solicitations quantity two (2)</i>
4	Vendor Selection*** & GRC Tool Technical Implementation by GRC Vendor***	*** Out of Scope for IBM	<i>A.2.2.5 Implementation of governance tool – *** dependency on WVOT, GRC Vendor, and selected GRC Tool</i>
5	Program Rollout Planning	<ul style="list-style-type: none"> • Program roll-out plan • High level training sessions for users on use of the governance tool (up to two 1-hour sessions) 	<i>A.2.2.6 Agency roll-out plan</i>

Phase		Typical Outcomes / Program Deliverables	Mapping to RFP Milestones
6	Program Operating Model Support	<ul style="list-style-type: none"> Operational Model for Cyber Risk Program based on a charge-back model 	<i>A.2.2.7 Policies and operations procedures</i>
7	Governance and PMO	<ul style="list-style-type: none"> Communication plan Periodic Project Status meetings (e.g. monthly, biweekly, etc. as needed) Support contact matrix / escalation matrix (detailing on-site support for major milestones and project initiatives) 	

2.3 Proposed Engagement Timelines

IBM's proposal will be delivered over the following time duration illustrated in the figure below.

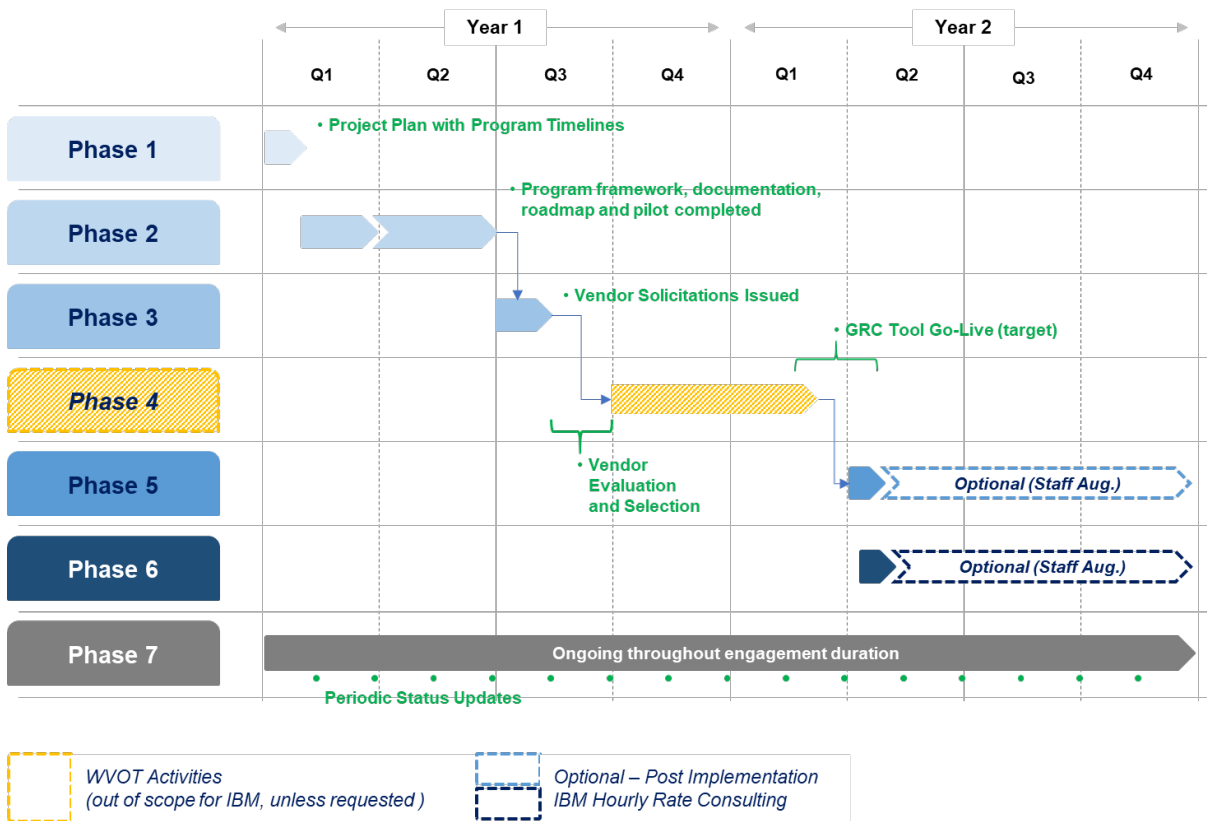


Figure 3: Proposed Engagement Timelines

Based on our experience with building similar programs, the target duration for each phase is estimated as shown in the table below:

Phase	Estimated Duration
1 Project Initiation and Program Planning	5 weeks

Phase		Estimated Duration
2A	Program Design and Framework Development	6-8 weeks
2B	Program Documentation, Pilot, and Finalization	12-13 weeks
3	Two (2) Vendor Solicitations	5-6 weeks (approx. 3 weeks for each)
4	Vendor Selection, GRC Tool Implementation by GRC Vendor, Assessment Vendor Onboarding	Estimated 6-8 months ***Out of Scope for IBM
5	Program Rollout Planning	3-4 weeks
6	Program Operating Model Support	3-4 weeks
7	Governance and PMO	Ongoing throughout engagement duration

2.4 Team Composition / Delivery Model

IBM Security strives to be WVOT’s trusted advisor and partner to help realize your vision and desired operating model for the CSRM. We have identified a delivery model including a team of proposed dedicated resources that is committed to your continued success.

As your trusted security partner, IBM will act as an extension of your security organization providing the following “layers” of resources, as further illustrated in the figure below:

- i. *Executive Leadership* – IBM Security executives involved throughout the duration of the engagement to oversee overall strategy, thought leadership, direction, and ongoing delivery excellence.
- ii. *Governance and Program Management Office (PMO)* – IBM Security delivery manager (engagement lead) and project management support personnel, to keep the engagement on track and on budget.
- iii. *Technical Delivery Team* – IBM Security consultants and analysts for day-to-day delivery of the CSRM program.

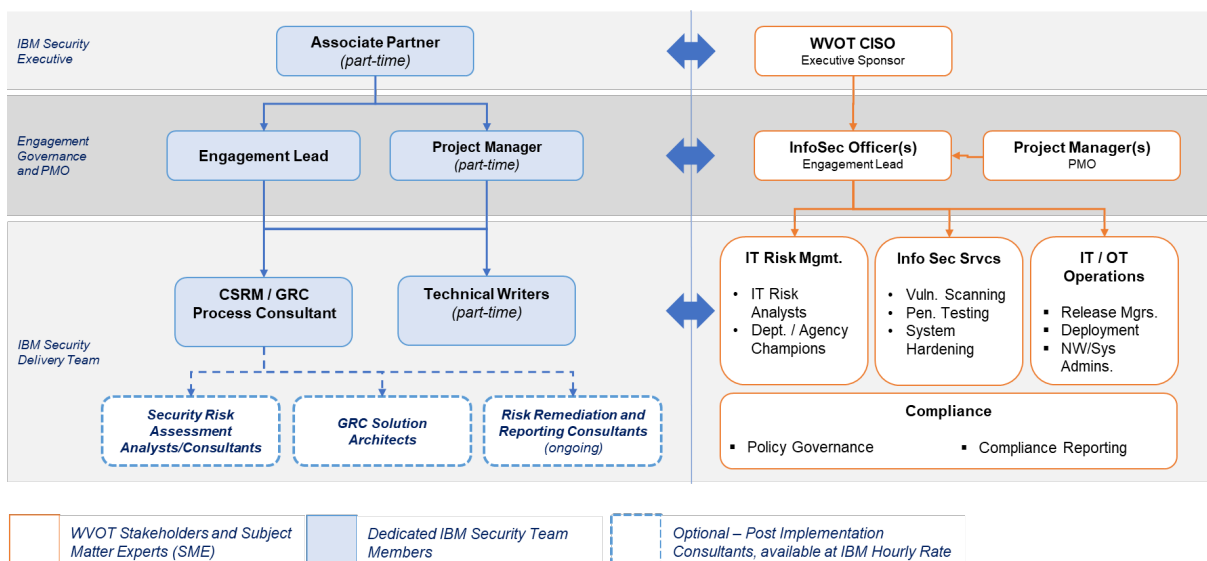


Figure 4: Delivery Model

2.5 Scope Definition and Related Assumptions

IBM's proposal is based on the following scope and assumptions. Please note that, any desired changes or enhancements to this scope can be discussed and mutually agreed upon by IBM and WVOT through subsequent discussions.

1. Based on our vast experience with both developing as well as running ISRM programs across a wide variety of clients, we understand that the term “risk assessments” may be used broadly to apply to assessments conducted on enterprise applications, systems and network infrastructure, critical shared services, data centers and operating facilities, OT environments, third party vendors and suppliers, cloud security providers (CSP), potential mergers and acquisitions, etc. Our proposal does not, currently, explicitly differentiate between these various types of assessments. Rather, we have proposed that these types and numbers of assessments will be documented and formalized as part of the Program build (Phase 2).
2. For purposes of Risk Profile determination of departments and agencies, a pilot set of up to 5 will be selected and agreed upon with the Client. The pilot set will include samples where contextual data / metadata is easily available or obtainable.
3. For purposes of Risk Assessment pilot, a pilot set of one large and one small agency will be selected. Further a pilot set of 3 applications and/or infrastructure systems will be selected and agreed upon with the Client. The pilot set will include samples where contextual data and conceptual, operational, and technical information is easily available.
4. IBM will partner with WVOT to determine the best, most reasonable ratio for required onsite presence versus remote work for our consultants.

3. Detailed Statement of Work

This section provides a description of services that IBM will fulfill, including key activities, completion criteria, and deliverables based on the high-level approach described above.

Note: [Text in blue font denotes references to the original RFP requirements.](#)

Phase 1: Project Initiation and Program Planning

The purpose of this activity is to finalize the project team members, develop a common understanding of the project objectives, roles and responsibilities, and assess West Virginia Office of Technology (WVOT) readiness to implement the Services by confirming that the appropriate information is documented.

IBM will facilitate a project initiation meeting on a mutually agreed date and time which will include:

- Identify key client stakeholders
- Introduce the IBM project participants;
- Discuss project team roles and responsibilities;
- Review the project methodology and objectives;
- Provide an overview of the project methodology; and develop the high-level project plan based on the phased approach outlined in this RFP response.
- Develop a preliminary schedule of activities and define the agenda for the Cyber Risk Program design workshop with West Virginia Office of Technology (WVOT) and IBM attendees.
- Develop and document the program charter.
- Develop a high-level target operating model.
- Review with key stakeholders and obtain consensus.

Completion Criteria: This activity will be complete when West Virginia Office of Technology (WVOT) has approved the proposed methodology.

Deliverables/Outputs:

- Kick Off Presentation
- Workshop Agenda
- Cyber Risk Program Charter
- Target Operating Model

[RFP Requirement:](#)
4.2.1.1 Framework Development

Phase 2A: Program Design and Framework Development

The purpose of this activity is to develop a customized ITRM Framework for WVOT along with the core set of foundational elements and building blocks needed for the program to ramp up and Go-Live.

IBM will:

1. Define and develop the following, at a minimum:
 - a) Target operating model depicting activities, roles, escalation points, and repositories
 - b) Listing of all parties to be directly involved (responsible, consulted, or informed) in ITRM functions at WVOT.
2. Outline a proposed enterprise framework for IT Risk Management, aligned with industry standards and best practices (for e.g. derived from one of NIST 800-39, ISO 27005, COBIT 5, etc.) and discuss preferred model with Client. This framework will address people, process, and technology requirements within the following main areas:
 - a) Risk Identification and Evaluation (Assessment)
 - b) Risk Treatment and Response (Remediation)
 - c) Risk Reporting and Communication
 - d) Risk Review and Monitoring

3. Review program details with WVOT to garner agreement on approach, and to confirm that the program will account for the standardization of the impact risk variable
4. Conduct a workshop with key WVOT stakeholders to discuss risk assessment methodologies and gain consensus on an approach. Goal is to review various risk assessment methodologies and gain consensus on an understandable & repeatable process and methodology.
5. Request and obtain an inventory of all enterprise systems (including applications, server and endpoint systems, network infrastructure, shared services, and data centers) that need to be in scope for the ITRM program. Work with Client to request and obtain business context data and metadata (such as asset owner, location, number of users, BIA scores, etc.)
6. Develop a formal, standardized, enterprise process customized for WVOT based on industry standards, which outlines the following at a minimum:
 - a) Overall process flow and high-level description of activities within each phase of the risk management framework, including: identification, risk analysis and rating, remediation planning and decision making, remediation execution, validation and closure.
 - b) Roles and responsibilities along the process (using, for e.g., a RACI assignment matrix).
 - c) Frequency and timelines associated with risk assessment and remediation process.
 - d) References to supporting artifacts, templates, worksheets.
7. Establish and document a risk profile mechanism that can be used to conduct initial inherent risk triage on agencies, using a tier model
8. Develop a Risk Profiling Procedure based on sensitivity of the agency's information, type of third parties they do business with, as well as inter agency operation (for example). Approach to be validated by WVOT
9. Perform pilot of Risk Profiling Procedure.

Completion Criteria

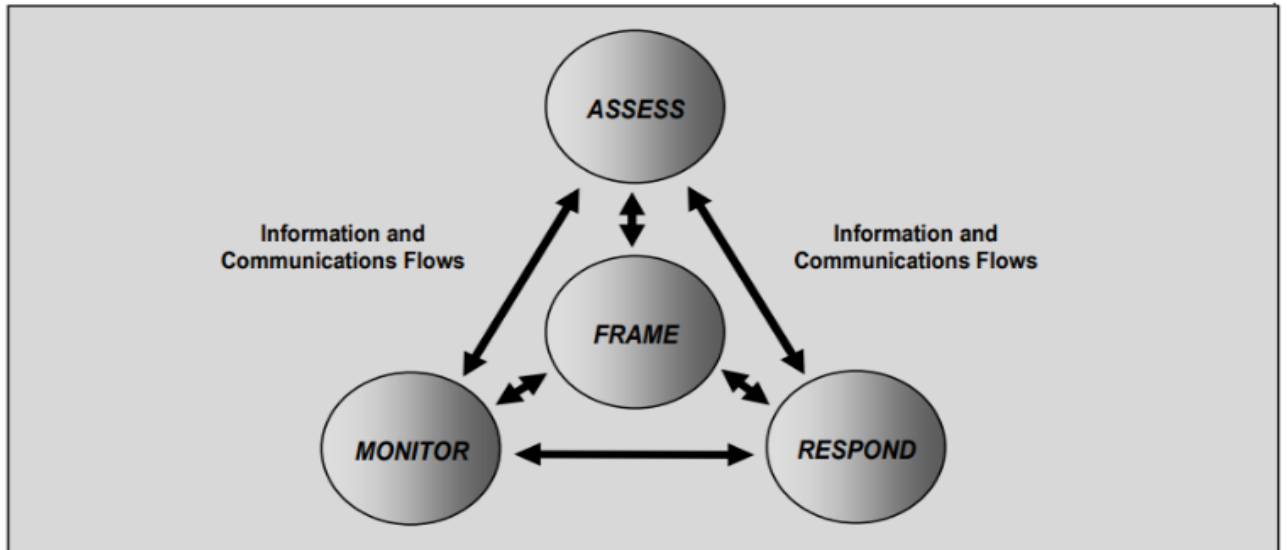
This activity will be complete when IBM has provided a preliminary ITRM framework to WVOT.

Deliverable Material

- Preliminary ITRM framework
- List of identified state entities (up to 5) for pilot
- Project timeline with key goals and objectives
- Target operating model selection to support 3-tiered organizational hierarchy
- Risk Profiling Procedure Development
- Completion of Risk Profiling Pilot

References

The overall risk management framework could be based on the following construct from NIST 800-30, as an example.



RFP Requirement:

4.2.1.2 Cyber Risk Program documentation/Creation

Phase 2B: Cyber Risk Program Documentation/Creation

1. Review various models in consultation with WVOT and agree upon the target model for the program build. For example, the 3-Tiered Risk Management Approach outlined in NIST SP 800-39.
2. Establish and document a risk analysis / assessment / calculation methodology based primarily on a qualitative approach (use of quantitative risk assessment approaches can be discussed and partially incorporated, if requested).
3. The process for collection, identification, categorization, prioritization, and mapping of risks will be established to align with organization's business objectives and strategy.
4. Identify a list of supporting artifacts to be developed and maintained. Examples include: templates for Risk Evaluation Worksheet, Risk Remediation Action Plan, Risk Register.
5. Identify and document Client specific standards and/or service level objectives (SLO) associated with the above processes. For example, this may include standards for risk rating, remediation SLO for high-risk items, risk ownership and sign-off, risk acceptance or transfer, etc.
6. Conduct one workshop to socialize the above IT Risk Management framework with key personnel from Client Information Security team:
 - a) Socialize the proposed IT Risk Management process,
 - b) Facilitate consensus on proposed roles and responsibilities.
7. Propose establishing an IT Risk Steering Committee / Forum that will oversee all IT risk decisions. Collaborate with WVOT to identify the appropriate parties for establishing an ITRM Steering Committee.
8. ITRM Framework will include the following, at a minimum:
 - a. Risk ranking model
 - b. IT risk register template (with risk reference library)

- c. Risk Assessment questionnaire(s)
- d. Risk Assessment process workflow

Deliverables/Outputs:

- Creation of fully documented Cyber Risk Program
- Develop & document Policies and operations procedure
- Develop reporting templates
- Develop program roadmap
- Roles and responsibilities between central teams and agencies
- Documented approach for agencies to apply framework and manage audit and assessment activities
- Pilot program Assessment results
- Document lessons learned from Pilot program.

RFP Requirement:

4.2.1.3 Compliance Audit Solicitation

Phase 3A: Compliance Audit Solicitation

The purpose of this activity is to assist WVOT in developing solicitation for Third party Compliance Audit. IBM will:

- Conduct market research to define the specifications and goals needed to create a solicitation that will allow agencies a procurement means to have a third party evaluate their adherence to security standards.
- Provide expertise in identifying, analyzing and evaluating agency risk and applying the appropriate security controls based on best practices
- Review vendor responses for suitability and provide advice to WVOT reviewers
- Provide consultation on an as needed basis to WVOT to assist agencies in using the solicitation

Completion Criteria: This activity will be complete when IBM has developed and documented the Compliance Audit solicitation in conjunction with WVOT and provided the final Compliance Audit Solicitation for issue to WVOT.

Deliverables/Outputs:

- Document specifications and goals based on market research for third party evaluation of agency adherence to security standards
- Aid WVOT in developing Compliance Audit Solicitation
- Perform and document review of Vendor response(s)
- Provide guidance and assistance to WVOT to assist agencies in using the solicitation via process development

RFP Requirement:

4.2.1.4 GRC Tool Solicitation

Technical implementation of GRC tool is out of scope – to be performed by GRC vendor

Phase 3B: Governance, Risk, & Compliance (GRC) Tool Solicitation:

The purpose of this activity is to Assist WVOT in developing solicitation for the Governance, Risk, & Compliance (GRC) Tool. IBM will:

- Assist WVOT in developing a solicitation for a GRC tool.

Completion Criteria: This activity will be complete when IBM has developed and documented the Governance, Risk, & Compliance (GRC) Tool solicitation in conjunction with WVOT personnel and completed the activities in the Deliverables/Outputs list below.

Deliverables/Outputs:

- GTC Tool Solicitation document (reviewed and approved by Client)

RFP Requirement: 4.2.1.5 Full Implementation

Phase 5: Program Rollout Plan:

The purpose of this activity is to Assist WVOT in the post implementation of the GRC tool by developing baseline security and use procedures, risk management policies and procedures, development of training and training of users - for the Governance, Risk, & Compliance (GRC) Tool. IBM will:

- Establish agreed upon baseline security and use procedures for the GRC tool.
- Develop baseline security and use procedures customized to state specific requirements
- Develop Risk Management policies and procedures
- Develop GRC tool training
- Train GRC tool users
- Develop and document the following program level artifacts to advise WVOT on a rollout plan:
 - Communications plan
 - Education and enablement of tools
 - Method to incrementally expand the pilot program
 - Plan for framework deployment and audit execution across the enterprise (Including the performance of audit of enterprise services)
- Develop high-level method for WVOT to support agencies with utilizing the third-party vendor that was awarded the contract to perform third party assessments

Completion Criteria: Completion of roll-out plan. Approval of plan by WVOT

RFP Requirement: 4.2.1.6 Ongoing Support

Phase 6: Ongoing Support

The purpose of this activity is to provide Ongoing support. IBM will:

- Develop a financial rates model to cover the projected operational expenses of the Cyber Risk Program based on the current agency charge-back model.
- The fee basis for this model will be based on the size and scope of the customer agencies as well as nature of risk services being requested.
- Collaborate with and assist WVOT in establishing pricing for various aspects of the Cyber Risk Program.

Completion Criteria: Chargeback model development and documentation. Approval of model by WVOT

Deliverables/Outputs:

- Development of a financial rates model to cover the projected operational expenses of the Cyber Risk Program based on a charge-back model

[RFP Requirement:](#)

4.2.1.7. Communication

Phase 7: Communication Plan / Governance and PMO

The purpose of this activity is to provide a clear communication plan to provide regular communication and support. Phase 7 will run the span of the project. IBM will as part of “Phase 1” project initiation workshop, gain consensus and agreement from WVOT stakeholders on the following:

- Establish regular communications to discuss project status at a minimum of every two (2) weeks.
- Provide communication to different levels of stakeholders in a cadence as agreed to and in collaboration WVOT
- IBM will provide on-site support for major milestones and project initiatives.
- IBM agrees that the State can apply custom branding to all documents and materials

Completion Criteria: Governance and PMO activities will be ongoing throughout all phases of the project.

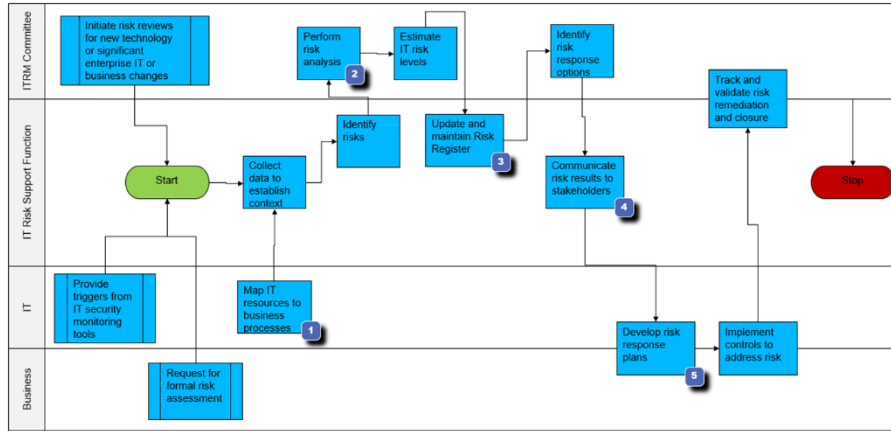
Deliverables/Outputs:

- Establishment of a clear communication plan
- Establishment of regular communication method to discuss project status at a minimum of every two (2) weeks
- Develop support matrix detailing on-site support for major milestones and project initiatives

Sample Deliverables (for illustrative purposes only)

Provided below are a few sample deliverables (sanitized) from prior similar work we have done.

A. *High-level Risk Management process workflow:*



1. IT Asset Inventory / Catalog
2. Risk Ranking Model
3. Risk Register
4. Risk Reporting and Dashboards
5. Detailed Remediation Action Plans

B. Sample RACI Chart for an ITRM Program (based on RiskIT framework):

ITRM Process ID	Risk IT No.	Key Activities	ITRM Support Function																	
			ITRM Committee	IT	Business Owners (I-DB)	CIO	Internal Audit	HR (?)	CFO	CEO	Board									
Risk Governance																				
RG1		Establish and Maintain a Common Risk View																		
	RG1.1	Perform enterprise IT risk assessment.	R	C	C	R	R	I												
	RG1.2	Propose IT risk tolerance thresholds.	C	R	C	A	A	C												
	RG1.3	Approve IT risk tolerance.	C	R	C	C	C	C												
	RG1.4	Align IT risk policy.	R	C	R	R	A	C												
	RG1.5	Promote IT risk-aware culture.	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	A
	RG1.6	Encourage effective communication of IT risk.	R	R	R	R	A	C												
	RG2	Integrate with ERM																		
	RG2.1	Establish and maintain accountability for IT risk management.																		
	RG2.2	Co-ordinate IT risk strategy and business risk strategy.																		
	RG2.3	Adapt IT risk practices to enterprise risk practices.																		
	RG2.4	Provide adequate resources for IT risk management.																		
	RG2.5	Provide independent assurance over IT risk management.																		
	RG3	Make Risk-aware Business Decisions																		
	RG3.1	Gain management buy-in for the IT risk analysis approach.	C	C	C	C	R	C												C
	RG3.2	Approve IT risk analysis.	C	A	C	R	C	I												
	RG3.3	Embed IT risk considerations in strategic business decision making.																		
	RG3.4	Accept IT risk.	C	R	C	A	R	I												I
	RG3.5	Prioritise IT risk response activities.	R	C	C	R	A	I												I
Risk Evaluation																				
	RE1	Collect data																		
	1.1	Establish and maintain a model for data collection	R	C	C	C	A	I												
	1.2	Collect data on the operating environment	C	C	R	R	A	I												
	1.3	Collect data on risk events.	R	C	C	C	A	I												
	1.4	Identify risk factors.	R	R	C	C	C	C												
	RE2	Analyze risk																		
	2.1	Define IT risk analysis scope	C	C	C	RA	C													
	2.2	Estimate IT risk	R	C	C	A	C													
	2.3	Identify risk response options	C	R	C	A	C													
	2.4	Perform a peer review of IT risk analysis																		
	RF3	Maintain risk profile																		

C. Sample Quantitative Risk Analysis / Scoring Worksheet (based on FAIR Methodology):

Response to WVOT RFP – Cyber Risk Program

Risk #		Risk Details		Incident Likelihood							Incident Impact				Risk and Value		
Assets Impacted	Sample Risk Register	Location of Incident	Attacker Tools (Means)	Ease of Exploit (BI/level of attack)	Exploit Availability	Target Attractiveness	Frequency of Attack (Historical/CS Log)	Probability	Likelihood	Attacker Motivation	Attacker Action	Likely Result	Detection & Containment Time	Impact	Unrecovered Time (Hours)	Security Maturity (Score)	
R1	Infrastructure	A threat agent attempts to gain unauthorized access (including virus infection) to the Organization IT IS Infrastructure by attacking a trusted server in the SCADA (OT) environment (20 computer ASAs servers).	United States (North America)	Information exchange	No modification needed (low BI/BI)	Google available	Highly Attractive	Event in top 10% attacks	40%	Moderate	Political gain	Authenticate	Loss of Information Integrity	Very Long	Minor	30.1	10/10
R2	Infrastructure	The Organization fails to ensure appropriate security procedures are implemented for computer networks.	Middle East	Suitor or Program	No modification needed (low BI/BI)	Google available	Highly Attractive	Event seen previously	94%	Highly Critical	Financial gain	Steal	Loss of Confidentiality	Very Long	Critical	94.0	2.0/10
R3	Infrastructure	The Organization fails to ensure appropriate security procedures are implemented for computer networks.	United States (North America)	Information exchange	Exploit exists, up-to-date (High BI/BI)	accessible in private lists	Medium Attractive	Event in top 1% attacks	3%	High	Political gain	Spoof	Loss of Information Integrity	Long	Major	8.3	10/10
R4	Infrastructure	A threat agent uses the Corporate IT IS Assets to create a denial of service attack against Operations components of the Organization.	United States (North America)	Physical attack	Exploit NA (Very High BI/BI)	No known exploits	Not Attractive	Event in top 1% attacks	2%	Unlikely	Damage	Probe	DoS: Availability, degradation of service	Short	Minor	0.8	10/10
R5	Infrastructure	An attacker uses the Corporate IT IS Assets to create a denial of service attack against Operations components of the Organization.	Africa	ToolKit	Exploit exists, up-to-date (High BI/BI)	Published in some private lists	Highly Attractive	Event in top 1% attacks	4%	High	Financial gain	Coax	Loss of Information Integrity	Medium	Major	36.4	10/10
R6	Infrastructure	An attacker uses smart TV to listen to the Organization's Boardroom conversations.	Eastern Europe	Information exchange	Exploit exists, up-to-date (High BI/BI)	accessible in private lists	Low Attractive	Event seen frequently	2%	Moderate	Financial gain	Disrupt	DoS: Availability, degradation of service	Very Short	Moderate	6.3	2.0/10
R7	Infrastructure	An attacker uses smart video conferencing to listen to the Organization's Boardroom conversations.	Africa	ToolKit	No modification needed (low BI/BI)	Google available	Not Attractive	Event in top 10% attacks	53%	High	Challenge, Status, Theft	Spoof	Loss of Confidentiality	Medium	Moderate	26.4	2.0/10
R8	Infrastructure	A threat agent attempts to gain unauthorized access to the Organization IT IS assets by gaining access by attacking a DNS Server.	Eastern Europe	Suitor or Program	Modification needed (low BI/BI)	accessible in private lists	Low Attractive	Event seen previously	44%	Moderate	Political gain	Authenticate	Theft of IT/ Data/PHN, Compromise	Long	Moderate	22.2	10/10
R9	Infrastructure	The Organization fails to deploy automatic equipment identification to help protect equipment.	Spain	Tool/Program	No modification needed (low BI/BI)	accessible in private lists	Not Attractive	Event seen frequently	7%	Moderate	Political gain	Steal	Loss of Confidentiality	Short	Minor	1.7	10/10

Risk #		Risk Details		Risk and Vulnerability Analysis Results					Loss Magnitude : Select						
Assets Impacted	Sample Risk Register	Detection & Containment Time	Impact	Unrecovered Risk Ranking	Security Control Maturity Levels (Select)	Treated Risk Ranking	Overall Risk Assessment	Lost Productivity	Expenses with Response	Expenses with Replacement	Regulatory Fines & Judgement	Loss to competitive advantage	Loss to Reputation	Mean Loss Magnitude (Calculated) (0-1000)	
R1	Infrastructure	A threat agent attempts to gain unauthorized access (including virus infection) to the Organization IT IS Infrastructure (for example ASA server).	Very Long	Major	30.4	10/Level	29.09	Low	Moderate (\$10K to \$100K)	Very Low (less than \$1K)	Very Low (less than \$1K)	Moderate (\$10K to \$100K)	Moderate (\$10K to \$100K)	Moderate (\$10K to \$100K)	\$70
R2	Infrastructure	The Organization fails to ensure appropriate security procedures are implemented for computer networks.	Very Long	Critical	94.0	2.0/Level	78.19	High	Moderate (\$10K to \$100K)	Low (\$1K to \$10K)	Significant (\$100K to \$1M)	Low (\$1K to \$10K)	Significant (\$100K to \$1M)	High (\$1M to \$100M)	\$4,729
R3	Infrastructure	The Organization fails to ensure appropriate security procedures are implemented for computer networks.	Long	Major	8.3	10/Level	7.88	Very Low	Very Low (less than \$1K)	Significant (\$100K to \$1M)	None	Low (\$1K to \$10K)	Very Low (less than \$1K)	Low (\$1K to \$10K)	\$54
R4	Infrastructure	A threat agent uses the Corporate IT IS Assets to create a denial of service attack against Operations components of the Organization.	Short	Minor	0.6	10/Level	0.65	Very Low	Very Low (less than \$1K)	Low (\$1K to \$10K)	Low (\$1K to \$10K)	Very Low (less than \$1K)	None	Low (\$1K to \$10K)	\$0
R5	Infrastructure	An attacker uses the Corporate IT IS Assets to create a denial of service attack against Operations components of the Organization.	Medium	Major	36.4	10/Level	34.90	Low	Very Low (less than \$1K)	Significant (\$100K to \$1M)	Low (\$1K to \$10K)	Low (\$1K to \$10K)	Very Low (less than \$1K)	Low (\$1K to \$10K)	\$240
R6	Infrastructure	An attacker uses smart TV to listen to the Organization's Boardroom conversations.	Very Short	Moderate	6.3	2.0/Level	6.59	Very Low	Moderate (\$10K to \$100K)	Low (\$1K to \$10K)	Low (\$1K to \$10K)	Very Low (less than \$1K)	Very Low (less than \$1K)	Low (\$1K to \$10K)	\$11
R7	Infrastructure	An attacker uses smart video conferencing to listen to the Organization's Boardroom conversations.	Medium	Moderate	26.4	2.0/Level	21.99	Low	Very Low (less than \$1K)	Significant (\$100K to \$1M)	Low (\$1K to \$10K)	Moderate (\$10K to \$100K)	Low (\$1K to \$10K)	Moderate (\$10K to \$100K)	\$249
R8	Infrastructure	A threat agent attempts to gain unauthorized access to the Organization IT IS assets by gaining access by attacking a DNS Server.	Long	Moderate	22.2	10/Level	21.29	Low	Very Low (less than \$1K)	Low (\$1K to \$10K)	Low (\$1K to \$10K)	Very Low (less than \$1K)	Very Low (less than \$1K)	Low (\$1K to \$10K)	\$7
R9	Infrastructure	The Organization fails to deploy automatic equipment identification to help protect equipment.	Short	Moderate	1.7	10/Level	12.71	Low	Very Low (less than \$1K)	Significant (\$100K to \$1M)	Low (\$1K to \$10K)	Low (\$1K to \$10K)	Very Low (less than \$1K)	Low (\$1K to \$10K)	\$33
em	Infrastructure	The Organization fails to ensure that diagnostic and maintenance equipment is protected against unauthorized access.	Very Short	Minor	1.4	10/Level	11.90	Low	Very Low (less than \$1K)	Low (\$1K to \$10K)	Low (\$1K to \$10K)	Moderate (\$10K to \$100K)	Very Low (less than \$1K)	Very Low (less than \$1K)	\$10

4. Qualifications and Experience

4.1 Representative Client Success Stories

IBM has an extensive and successful track record of working with Clients across multiple industry sectors and helping them with various aspects of their risk management programs, including assessments, risk ranking and reporting, controls testing and evaluation, remediation support and facilitation, etc. The following information describes Client case studies where IBM provided services like those being proposed in this document.

Note: IBM has a strict policy of not revealing actual customers' business details due to the sensitivity associated with such information unless we obtain a consent and approval from the customer in order to do so, and until we enter one-on-one discussions.

Client Case Study #1

<i>Client Profile</i>	Large North American financial services institution
<i>Client Requirement (Problem Statement)</i>	Client needed an assessment of their existing IT risk management framework and governance processes to validate if the supplier process is in sync with their IT Risk framework. Client sought IBM's assistance to remediate any gaps and develop an effective ITRM governance model.
<i>IBM Solution</i>	<p>IBM Security performed the following activities:</p> <ul style="list-style-type: none"> Analyzed the client supplier management framework, Supplier governance model and IT risk framework. Conducted a gap analysis for compliance and adherence of client's supplier management process to their IT Risk framework. Presented a gap analysis report to identify and prioritize high impact IT risk security gaps. Developed a detailed roadmap with maturity target timeframe with recommendations on how to remediate risks. Developed the ITRM governance model for supplier management. Developed monitoring activities for suppliers' noncompliance to client's IT risk policies and standards
<i>Client Benefits</i>	With the detailed gap analysis report from IBM, Client was able to prioritize gaps and build a structured ITRM governance model and associated processes, interactions, and reports.

Client Case Study #2

<i>Client Profile</i>	Large international airline serving more than 200 airports on six continents.
<i>Client Requirement (Problem Statement)</i>	Client needed assistance in designing and building leading Third-party Risk Management program and best practices for evaluating security and privacy risks when conducting business and exchanging data with their third parties.
<i>IBM Solution</i>	<p>IBM Security performed the following activities:</p> <ul style="list-style-type: none"> Developed a detailed project plan to establish a third-party risk management program and formalize related policies and procedures. Established a detailed third-party and third-party services inventory. Established an inherent risk stratification process (using a tier model).

	<ul style="list-style-type: none"> Established a cadence of ongoing monitoring of third parties based on inherent risk. Established third parties onboarding and termination process and procedures. Established Process for review of the contractual agreement including new contracts and contracts due for renewal. Automation of TPRM activities by integrating applicable TPRM source systems with the RSA Archer GRC solution. Included creating a repository in Archer for TPRM vendor records and supporting data. Developed relevant reports and executive dashboards for TPRM within the RSA Archer solution.
Client Benefits	By engaging IBM, the client established a broader third-party security program that enhanced its capability to manage and govern information security pertaining to third parties more effectively and efficiently. The client increased maturity in terms of overall vendor risk management practices.

Client Case Study #3

<i>Client Profile</i>	USA-based energy and utilities company
<i>Client Requirement (Problem Statement)</i>	Client engaged IBM Security ("IBM") to conduct an Information Security Assessment, with actionable recommendations and a focus on the NIST Cybersecurity Framework (CSF). The assessment was a technical review of client's capabilities to help support continuous improvement of the enterprise information security program.
<i>IBM Solution</i>	<p>IBM Security performed the following activities:</p> <ul style="list-style-type: none"> Conducted a comprehensive maturity and risk assessment of Client's security program against NIST CSF. Analyzed existing security program, controls, and capabilities and identify strength and weaknesses from people, process, and technology perspectives. Developed security gap analysis with rating system that measures the relative probability, threat, and vulnerability for the identified risk and decision tree (where applicable).
Client Benefits	Client got a set of prioritized recommendations and a roadmap to roll out initiatives and projects to address areas of highest risk.

4.2 Representative Consultant Profiles

We realize that the qualifications and experience of our professionals are extremely integral to the success of our consulting and professional services engagements for our Clients. As mentioned above, we have identified a team with required breadth and depth of our cyber security and risk management expertise.

Provided below are a set of representative consultant profiles; detailed practitioner resumes will be made available upon request.

David Schoenbrot, CISSP

 <p>David Schoenbrot Managing Consultant IBM Security Services dmschoen@us.ibm.com</p>	<p>Functional Expertise</p> <ul style="list-style-type: none"> • Governance, Risk, & Compliance • Security Program Development and Operation • Cybersecurity Assessment • Security Strategy & Roadmaps 	<p>Industry Experience</p> <ul style="list-style-type: none"> • U.S. Government • Healthcare • Manufacturing • Finance and Banking • Retail
<p>IBM Role</p> <ul style="list-style-type: none"> • Managing Consultant in IBM Security Transformation Services • 30+ years of Information Security and Information Technology services; Transformation, Strategy, Implementation and Operation; Governance, Risk, and Compliance; Assessments and Roadmaps; Staff Augmentation; Vulnerability Management; Data Privacy; Enterprise Security Architecture; Cloud Security • Clients include federal and quasi government organizations; Small through large companies seeking improved security or regulatory compliance; Healthcare and Regional Health Information Organizations (RHIOs); Electronics Manufacturing; Aerospace; Financial, Retail and Distribution. <p>Professional Education & Certifications</p> <ul style="list-style-type: none"> • BA Mathematic, State University of New York • CISSP 110884 • FISMA, HITRUST, MARS-E, NIST CSF, DFAR CUI, FedRAMP, FFIEC, ISO2700x, NIST SP800 series. 	<p>Experience & Notable Accomplishments</p> <p>Transformations – Led a three year effort for a federal government bureau to improve its security from failing to A performance. Co-developed and implemented a new distributed security governance (BISO) model for a fortune 100 company. Teamed with an organizational change specialist to assess stakeholder partnerships for a major investment firm security program leading to its re-organization</p> <p>Staff Augmentation – Provided vulnerability, threat and identity management services to a \$1.2B US Navy IT project; developed tools and methods used for years after the engagement. Developed HITRUST CSF 9.1 guidance and detailed and technical procedure for a State RHIO. Trusted advisor for a aerospace CFO and security-director on government contracts and regulatory requirements. Provided advisory services including NIST FISMA, NISPOM, DFARs, ITAR, FedRAMP and SP800-171.</p> <p>Assessments and Roadmaps – Banking NIST CSF, SBS and FFIEC in-depth assessment resulted in immediate corrective actions, creation of an integrated control set, and multi-year improvement roadmaps. Automotive industry NIST CSF, ISO 2700x and internal policy and procedure assessment, setting roadmap for the newly established US security office. Electronics Manufacturing NIST CSF global executive level focus.</p>	

IBM Security

IBM


Bill Kwak, CISSP

 <p>Bill Kwak Security Strategy, Risk & Compliance Consultant IBM Security Services bill.kwak@ibm.com</p>	<p>Functional Expertise</p> <ul style="list-style-type: none"> • Governance, Risk, & Compliance • Cybersecurity Assessment • Security & Program Management • Security Strategy & Operations • Security Architecture 	<p>Industry Experience</p> <ul style="list-style-type: none"> • Healthcare • Technology • Banking • Financial • U.S. Government
<p>IBM Role</p> <ul style="list-style-type: none"> • Security Strategy, Risk & Compliance Consultant • Security Architecture Consultant • 19 years of progressive experience in CISO advisory, Data Privacy, eDiscovery and Investigations, GRC, Incident Management, Security Audit Remediation, Security Strategy & Roadmap, and Cloud Security. • Performed strategy and risk analysis for healthcare, financial, banking, insurance and government sectors <p>Professional Education, Certifications, & Associations</p> <ul style="list-style-type: none"> • Wright State University – Master’s of Science • University of Akron – Bachelor’s of Science • CISSP • Board Member of Regional Cloud Security Alliance 	<p>Experience & Notable Accomplishments</p> <p>Major banking organization – Provide input and direction for security initiatives, provide guidance to multiple security towers to integrate services and products into customer environment, facilitate executive level discussions for security initiatives based on risk appetite, and design solutions to meet organization’s strategic roadmap.</p> <p>Large healthcare system – Performed medical device risk assessment evaluating over 100 unique device types by validating asset inventory, assessing technical vulnerabilities, reviewing manufacturer provided information, evaluating existing processes, determining compensating controls, and providing remediation roadmap to CISO and security team</p> <p>Major Financial Institution – Lead discussions to optimize security and operational workstreams to enhance and secure customer environment, design solutions to meet organization’s security roadmap, facilitate coordination of incident response efforts, work with internal audit to meet regulatory requirements.</p> <p>Recent Presentations and Speaking Engagements</p> <ul style="list-style-type: none"> – SecureWorld Philadelphia 2017: Security and Medical Devices – Villanova University 2017: State of Security Symposium 	

IBM Security

IBM

Jonathan Knapp, CISSP

 <p>Jon Knapp Senior Managing Consultant IBM Security Services jknapp@us.ibm.com</p>	<p>Functional Expertise</p> <ul style="list-style-type: none"> • Governance, Risk, & Compliance • ISO 27X Specialist • Cybersecurity • Program Management Consulting • Information Security Management 	<p>Industry Experience</p> <ul style="list-style-type: none"> • Financial Services • Life Sciences • Telecom • Manufacturing • Energy
<p>IBM Role</p> <ul style="list-style-type: none"> • Senior Managing Consultant focused on Governance, Risk and Compliance working with large multinational corporations. • Specialize in Security Program Assessments. • Jon's consulting experience spans 25 years with 19 years dedicated to global security consulting and leadership. He has successfully balanced business objectives and security/compliance requirements for industry leaders. • Past clients include Financial Services, Life Sciences, Telecom, Manufacturing, Health Care and Energy. <p>Professional Education & Certifications</p> <ul style="list-style-type: none"> • Berklee College of Music • CISSP #39940 • ISO 27000 Lead Auditor 	<p>Experience & Notable Accomplishments</p> <p>NYC Cloud based 911 Firm – Lead consultant on ISO 27001-2 Gap Assessment > Cloud based ISMS selection>Greenfield Security program & policy build. Subsequently, I performed the Internal ISO Audit in preparation for stage 1 & 2 ISO certification audit. Client subsequently received ISO 27001 Certification.</p> <p>Large International bank – Program Lead on concurrent FFIEC CAT (Cyber-Security Assessment Tool) and NYS DFS (23 NYCRR 500) Assessment.</p> <p>Global Life Sciences Manufacturer – Project & technical lead on a large global multi-site ISO 27002 Gap And Risk Assessment. This project included ISO Controls and Risk Assessment's with corresponding risk treatment plans. Sites assessed included operations in Michigan, New Jersey, California, Puerto Rico, India, Ireland and Germany under very tight moving time frames.</p> <p>Large US based bank - Complex project consisting of an ISO27002 Gap Assessment including multiple subsidiaries and affiliates, in parallel with FFIEC CAT Assessment.</p> <p>Leading global payment solutions client – Provided incident management service for the West Coast location in close co-ordination to an IBM peer located at the East Coast location in response to a targeted cyber breach. As result of the service, the client was able to contain, eradicate, and recover in organized manner and realize key security areas for improvements.</p> <p>Large US based bank – NIST 800-53 Controls Assessment.</p>	

9 IBM Security



Phil Park, CCSK, CISA, CISSP, PCIP, PMP

 <p>Phil Park Associate Partner IBM Security Services phil.s.park@us.ibm.com</p>	<p>Functional Expertise</p> <ul style="list-style-type: none"> • Governance, Risk, & Compliance • Cybersecurity Assessments • Cloud Security Strategy • Security Strategy & Operations • Third Party Risk Management 	<p>Industry Experience</p> <ul style="list-style-type: none"> • Banking & Capital Markets • Public Sector • Transportation • Healthcare • Oil & Gas
<p>IBM Role</p> <ul style="list-style-type: none"> • Associate Partner at IBM Security Strategy, Risk & Compliance • 20 years of experience in CISO advisory, Cloud Security, Data Security & Privacy, Enterprise Security Architecture, GRC, Incident Management, ISMS, PCI Advisory, Problem Bank Resolution & Receivership, Security Audit Remediation, Security Strategy & Roadmap, and Target Operating Models. • Past clients include Fortune 100 firms, global corporate & investment banks, and U.S. financial regulatory agencies <p>Professional Education & Certifications</p> <ul style="list-style-type: none"> • MBA, Strategy, University of North Carolina • MS, Information Systems Technology, George Washington University • BBA, Management Information Systems, University of Oklahoma • CBCP, CCSK, CGEIT, CISA, CISSP, ITIL, PCIP, PMP 	<p>Experience & Notable Accomplishments</p> <p>Global mass media client – Transformed client's AWS cloud security capabilities by providing baseline security requirements & controls, cloud security reference architecture assets, and cloud security strategy roadmap as part of SAP migration to the AWS.</p> <p>Large global bank client – Led independent validation & analysis of the client's existing NY State DFS 23 NYCRR 500 impact assessment, identified current state of the client's information security program maturity by leveraging CMM, and developed a strategic roadmap that provided solutions to the identified gaps including resource and cost estimations.</p> <p>Major US airline client – Provided enterprise security architecture advisory services that included the following: enterprise security architecture processes, security taxonomy, security reference architecture, security requirements, threat modeling, baseline security controls, DevSecOps checklist, API security, GDPR, architecture review board representation, and security metrics.</p> <p>Fortune 50 financial services client – Advised CISO on 3 year information security strategy to improve the alignment of the information security program with key business and technology initiatives (Cloud, Social, & Mobile) and supported risk reduction/mitigation and cost optimization efforts.</p>	

IBM Security



5. Key Success Factors

Based on IBM's vast and diverse experience across hundreds of Clients, the following is a list of factors that we believe will be critical to the success of WVOT's Cyber Risk Program.

1. ***Tone from the Top***

Executive sponsorship is critical to the overall success of an enterprise risk management and cyber security program. Honest communication, collaboration, and cooperation starts with the right message and direction from the top.

2. ***Business Unit- / Department- / Agency-level Buy-in and Accountability***

All business units should work together with the WVOT group in order to strengthen the overall security posture; the Cyber Risk Program representatives must have a seat at the table early in the IT decision-making process.

3. ***Standardized Risk Management Framework***

A formal, documented, approved, and published ERM / ITRM / CSRM framework is an integral part of any organization's cyber security program. This framework should include standardized definitions for risk levels, acceptable risk thresholds, key risk indicators, risk reference libraries, IT Risk Register, etc. so that everyone is using the same language.

4. ***Risk-Aware Culture***

People are (still) the weakest link within cyber security; it is critical to educate the workforce at every level to realize a balanced, effective, and risk-based cyber security program across the enterprise.

5. ***Ongoing Measurement and Continuous Improvement***

While a number of IT projects/initiatives are being implemented, are in flight, or are being planned at any given point of time, the risks associated with these projects/initiatives need to be monitored on an almost ongoing basis in order to provide management with the right data points that they need to make key enterprise risk decisions.

In Summary

In summary and along the lines of the above guiding principles, we strongly believe that we have designed a strategic and holistic engagement approach to help WVOT with this strategic initiative. We would welcome the opportunity to further review and elaborate on our proposal to you.