Response to Request for Sealed Proposal:
Information Technology (IT) Risk Assessment
#22031819
PACKET 1

Contact for RFP Response:

Paul Ashe
pashe@securanceconsulting.com
Office: 877.578.0215
Direct: 913.758.2532
Fax: 813.960.4946

Corporate Office:
Securance Consulting
6922 W. Linnebaugh Avenue
Suite 101
Tampa, FL 33625
www.securanceconsulting.com

Project Office:
Securance Consulting
183 N. Stetson Street
Suite 3500
Chicago, IL 60601
www.securanceconsulting.com

Schedule 70 Contract GS-35F-0583X
Schedule 520 Contract GS-23F-0076X
# Table of Contents

Packet 1

**Introduction**
Letter of Transmittal ........................................... 2

**State of Illinois Request for Sealed Proposals,**
IT Risk Assessment #22031819,
Section 1 .................................................................... 5

**Offeror’s Proposed Solution to Meet the State**
of Illinois’ Requirements

**Proposed Scope**
Understanding of Scope .................................. 23

**Approach and Methodology**
IT Audit .......................................................... 26
Application Security Assessment ......................... 29
Web Application Testing .................................. 30
Network Architecture Review .................................. 32
Firewall Review .................................................. 33
Policies and Procedures Review .............................. 34
Audit Program .................................................. 35
Documentation Standards ...................................... 36

**Project Management**
Project Management .................................. 37
Information Sharing Security .................................. 38

**Related Experience**
Related Experience ........................................... 40

**Timeline, Milestones and Deliverables**

**Proposed Project Timeline**
Proposed Timeline ........................................... 42
Gantt Charts
Staffing Plan .................................................. 43
Sample Deliverables ........................................... 47

**Offeror I Staff Specifications**

**Offeror Qualifications**
Offeror Qualifications ........................................... 48

**Staff Qualifications**
Staff Qualifications ........................................... 51

**The Next Step**
What to Expect ........................................... 62
The Next Step ........................................... 63

**Appendix A: Sample Deliverables**
Sample Status Report

---

This proposal contains confidential material proprietary to Securance Consulting. The material, ideas and concepts contained herein are to be used solely and exclusively to evaluate the capabilities of Securance Consulting to provide assistance to the Illinois State Board of Education ("ISBE"). Any services Securance Consulting may provide to the ISBE will be governed by the terms and conditions of a separate written engagement agreement signed by both parties. All offers to provide professional services are valid for ninety (90) days.
Letter of Transmittal

Securance Consulting is a professional services firm dedicated to IT security, internal audit risk consulting and compliance. We were founded in 2002 by a group of former “Big 4” risk consultants. Their idea was to create a firm of Senior IT Security Consultants that would provide high-quality consulting services without a high overhead. Our independence and experience mean that clients receive objective, pure advice. Securance has a unique firm structure, which is supported by these points: Efficiency, Knowledge of the industry, Qualifications, Expertise and Quality Control.

In Securance, you will find a team with a passion for helping you manage IT risk, a service plan that is aligned with your priorities and a level of responsiveness that will continually reflect our commitment to you and your organization. This engagement will be a collective effort. Common goals, cooperation, teaming, talent, personal leadership, speed, creativity and a shared definition of value will define our relationship. Responsibilities will be clear, and our commitment to helping you achieve your goals will be evident. Together, we will significantly improve your organization's IT security posture. When you partner with Securance, you can expect the following:

Expertise
Our firm specializes in IT security, IT internal controls and IT risk management. Since our inception in 2002, we have performed IT services for numerous public sector organizations, including educational institutions. We have performed many engagements similar in scope to the project that the Illinois State Board of Education (ISBE) has requested. Organizations that trust Securance as their IT risk management partner include: the Teachers' Retirement System of the State of Illinois; the University of Kentucky; Frederick County, Maryland, and Frederick Community College; Houston Community College; Louisville – Jefferson County Metro Government; the Ohio Public Employees' Retirement System; and many more.

We will not be learning on the job! We are EXPERTS already.

Staff
We propose a team of IT security professionals who maintain the following certifications:
- CISA - Certified Information Systems Auditor
- CISSP - Certified Information Systems Security Professional
- CPA - Certified Public Accountant
- SANS - IT Security Training I Certifications

We understand technology and all facets of IT security. We can identify and remediate any IT security weakness. In addition, our consultants continually train to remain current in IT security trends and techniques. Each Senior IT Consultant will have a minimum of 10 years' experience.
Summary Understanding of Project Scope
We have reviewed the RFP issued by ISBE and, based on our understanding of the scope of requested services, believe that the following is an accurate summary of the project to be performed:

Phase I: Implementation and Information Gathering
- Project Planning
- Information Gathering
  - Conduct interviews with key personnel:
    - Gain an understanding of network architecture, systems and IT processes.

Phase II: Analysis
- IT Risk Assessment, Including:
  - Application security reviews of key application systems:
    - Student Information System (SIS) and Illinois Longitudinal Data System (ILDS);
    - Teacher Information Systems – Educator Licensure Information System (ELIS) and Employment Information System (EIS); and
    - Illinois Interactive Report Card (IIRC);
  - Assessment of ISBE Web Application Security (IWAS);
  - Comprehensive network architecture review;
  - Firewall reviews;
  - Policies and procedures review; and
  - Formulate recommendations regarding ISBE’s IT Security Awareness and Training Program.

Phase III: Reporting
- Final Deliverables
  - IT Risk Assessment Analysis Report;
  - Recommendations Regarding the Development of an IT Security / Awareness Training Program;
  - Recommendations for Changes to IT Security Policies and Proposed Language for New Policies;
  - Risk Mitigation Plan; and
  - Electronic Copy of Executive Summary.

Phase IV: Presentation
- Executive Summary Presentation
  - Executive Summary Presentation; and
  - Question-and-Answer Session.

Remediation
We guarantee a comprehensive IT risk assessment and deliverables that include all details necessary to immediately implement full remediation. Our team is composed of former “Big 4” IT security consultants; we know what it takes to build a well-controlled IT environment.

Delivery Report
We guarantee that we will deliver all services within a mutually agreed-upon time frame. We will complete the entire project in six (6) months or less. Furthermore, you will not have to wait for our reports. We issue draft reports one (1) week after concluding fieldwork.
Fee Structure
Securance is a firm of Senior IT Security Professionals. Our fee structure is simple: one hourly rate for all seasoned consultants. We will absorb all travel-related expenses associated with this engagement.

No other firm can offer the combination of skilled consultants, a fresh perspective, IT security expertise and cost value that Securance is offering you. These are the factors that set Securance apart from its peers.

Professional regards,

Paul Ashe, CISA
President & Sr. IT Audit | Security Consultant
Securance Consulting
SECTION 1 - SPECIFICATIONS/QUALIFICATIONS/STATEMENT OF WORK

1.1. GOAL:
The Illinois State Board of Education (ISBE) seeks to engage the professional services of an independent, qualified vendor to conduct a multi-phased Information Technology (IT) policy, program and architectural Risk Assessment to identify risks, create a sound policy foundation and develop a mitigation plan covering privacy, confidentiality and security practices of student, employee and educational data systems. During the Presentation Phase, the vendor will make recommendations to key ISBE personnel that cover governance, security plans, policies and procedures; system and applications architecture review; risk management and information security programs; and technical, management and operational security controls.

ISBE anticipates that the entire project's duration be no longer than six months.

1.1.1. BACKGROUND

ISBE is reliant on electronic infrastructure. There are over 150 applications, networks and interconnections to local education agencies (LEAs), schools, universities and nonprofits. In recent years, ISBE has internally developed critical systems that collect and store confidential information at the district-, school-, educator- and student-level, and is currently engaged in a large project to develop and host a statewide longitudinal data system (LDS). The LDS is intended to be used by a variety of constituents that also includes a public-facing view of its data. ISBE's security and protection of private and confidential data is a paramount responsibility. The vendor will provide recommendations to ISBE for necessary revisions of existing and/or formulation of new IT controls that specifically address any policy, practice, management, operations, infrastructure, application, network and/or architectural areas of risk that are identified.

1.1.2. OVERVIEW

ISBE's intent is to have well-designed and well-managed controls that protect its information technology network with effective computer/infrastructure/network/hardware/software security controls that provide for safeguarding, securing, and controlling access to hardware, software and personal confidential information stored in its computer system.
To that end, the vendor will perform a risk assessment in accordance with an accredited methodology such as that prescribed by the National Institute of Standards and Technology (NIST), International Electrotechnical Commission (IEC) or other accredited methodologies with ISBE management approval. The vendor will include an assessment of potential vulnerabilities in 1) unauthorized disclosure of data, 2) unauthorized modification of its system/network/applications, its data or all of these, and 3) denial of service, access to data or both to authorized users.

As described herein (and detailed in Section 1.4) the vendor will design, implement, manage and report on an ISBE IT Risk Assessment project. The vendor is responsible for all costs for on-site resources to perform this task on the days the vendor is present at ISBE facilities and the vendor agrees that ISBE will pay no travel or accommodation charges.

ISBE suggests four basic project phases as follows, but will consider recommendations for other project designs and structures. (Authorized ISBE signature is required for satisfactory completion of each phase.)

   Phase I: Implementation and Information Gathering
   Phase II: Analysis
   Phase III: Reporting
   Phase IV: Presentation to ISBE

ISBE will designate an internal coordinator to facilitate site interviews, all ISBE meetings and ISBE management approvals/signatures. The vendor will provide a project manager for this specific project. It is acceptable to ISBE that during the course of the project, specific phases may overlap. Key vendor personnel, including the project manager, will be expected to conduct a sufficient number of on-site meetings with ISBE staff to discuss in detail each component of the analysis, results and resolution of any outstanding issues. The vendor will prepare agendas for all joint meetings.

The vendor will provide a thorough analysis of, among other things, policies, practices, operations, controls, physical work space needs and resources of the various IT teams, including infrastructure; architecture; computer operations; programming; system dependencies; servers; storage; data warehousing; file transport; point-to-point videoconferencing; recording and hosting of webinars; online go-to-meetings; software licensure; virtualization; and the deployment, repair, and maintenance of PCs, laptops, wireless devices, printers, scanners, etc. The analysis will address sensitivity, threats, vulnerabilities, defined risks, controls and safeguards. As approved by ISBE management,
this work can be conducted on-site at ISBE's Springfield office and/or off-site at the vendor's facilities.

The vendor will dedicate sufficient time for its qualified and well-experienced security and risk assessment specialists to perform a complete analysis for the IT Risk Assessment, and will create a set of reports and recommendations in accordance with risk assessment industry standards and in similar scope and format as identified herein. The vendor will document recommendations to identify the gap(s) between ISBE's current position (the likelihood of risk), the existence and effectiveness of ISBE's current controls, and where ISBE needs to safeguard against risk exposure. In addition to providing risk level definitions, gap findings and analysis of current risk exposure, the report and recommendations will:

- Identify operational, technical, management and other vulnerabilities that are exploitable by both internal and external threats that are intentional and unintentional;
- Offer proven best practices and safeguards (security features, policies, practices and controls) that when added to ISBE's current IT environment, mitigate the risks associated with operations to a manageable level; and
- Evaluate the confidentiality (protection from unauthorized disclosure of system data information), integrity (protection from improper modification of information) and availability (loss of system access) of the system.

The vendor will host a formal presentation at ISBE's Springfield office that will represent an Executive Summary for the IT Risk Assessment. Based on the reports, the vendor's presentation will identify recommendations, existing policies, practices, safeguards and controls that need improvement, and will also contain new policies, practices, safeguards and controls recommended as may be needed to hold exposure of operations to a manageable level.

All documentation (in any format) is considered the property of ISBE, will be maintained by the vendor, must be available for reference by both parties throughout the duration of this project and surrendered to ISBE at the project's completion.*

*Note: All work performed, notes taken, diagrams, reports generated or supplies created by the vendor under this contract, whether written documents or data, goods or deliverables of any kind, shall be deemed work-for-hire under copyright law and all intellectual property and other laws, and ISBE is granted sole and exclusive ownership to all such work. ISBE shall own all rights, title and interest to
any generic components to the Custom Work Product. The vendor shall sign such
documentation as may be reasonably requested by ISBE to insure that title is vested
in ISBE. Vendor hereby assigns to the State all right, title and interest in and to such
work including any related intellectual property rights, and waives any and all
claims that the vendor may have to such work including any so-called "moral rights"
in connection with the work. Vendor acknowledges that ISBE may use the work
product for any purpose. Confidential data or information contained in such work
shall be subject to confidentiality provisions of this contract.

At no point in this project will any "phase" be considered completed without the authorized
signatures of both parties.
The ISBE coordinator will host any and all policy development meetings needed and upon
their conclusion, ISBE should have both newly recommended, revised and crafted policies,
practices, controls and safeguards that are the result of the IT Risk Assessment. ISBE's
adoption and implementation of revised policies, new policies, recommended processes
and procedures, application/software/infrastructure modifications, and other actions will
take place following the completion of the project's final phase.

1.2. SUPPLIES AND/OR SERVICES REQUIRED:

As described later herein, penalties may be taken against the vendor's total invoice for each phase
of the project not completed by the date specified in the finalized project plan/timeline.

<table>
<thead>
<tr>
<th>Category: Work Plan</th>
<th>Scoring Criteria: Proposal reviews will be based on the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total 540 Points Possible</td>
<td>• (350 PTS) Vendor should provide a thorough project plan and supporting documentation including, but not limited to:</td>
</tr>
<tr>
<td></td>
<td>➢ Project clarity and overall organization;</td>
</tr>
<tr>
<td></td>
<td>➢ Precisely defined project phases;</td>
</tr>
<tr>
<td></td>
<td>➢ Justification for established project phases;</td>
</tr>
<tr>
<td></td>
<td>➢ Concise identification of all tasks &amp; objectives;</td>
</tr>
<tr>
<td></td>
<td>➢ Identification of activities to complete tasks &amp; objectives;</td>
</tr>
<tr>
<td></td>
<td>➢ Identification of all task dependencies;</td>
</tr>
<tr>
<td></td>
<td>➢ Alignment of identified resources to accomplish tasks, complete objectives and meet milestones and timelines;</td>
</tr>
<tr>
<td></td>
<td>➢ Identification of possible project roadblocks;</td>
</tr>
<tr>
<td></td>
<td>➢ Total plan duration; and</td>
</tr>
<tr>
<td></td>
<td>➢ A complete staffing plan for each phase including all task owners.</td>
</tr>
<tr>
<td><strong>Timeline, Milestones and Deliverables:</strong> Total 180 Points Possible</td>
<td><strong>Vendor should submit a complete timeline for each project phase and for the entire project. The timelines should include:</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| **(80 PTS)** Use of accredited methodology/work approach  
  ➢ Justification for methodology/work approach  
  **(110 PTS)** Comparison/correlation to past projects of similar size and scope | ➢ Identification of all tasks and milestones;  
  ➢ Staffing or person(s) responsible for tasks and milestones' completion;  
  ➢ Timeline detail: providing start date, work days to complete and end date for each task and work phase;  
  ➢ Feasibility of timelines and milestones – realistic targets;  
  ➢ Identification of all milestone & timeline dependencies; and  
  ➢ Ability to complete the entire project within a six-month, or shorter, time frame. |
| **(110 PTS)** Itemization of all deliverables and staff responsible for delivery  
  ➢ Realistic due dates for each deliverable | ➢ Realistic due dates for each deliverable |
| **(15 PTS)** Description and examples of weekly progress reports and task lists | |

1.3. **OFFEROR’S PROPOSED SOLUTION TO MEET THE STATE’S REQUIREMENTS:** Please either respond in the space below or in the following prescribed format: Microsoft Word 2007 or a later version.

Please see attached pages.

1.4. **TIMELINE, MILESTONES AND DELIVERABLES:**

ISBE seeks the vendor’s expertise in establishing the appropriate timeline for completion of the IT Risk Assessment. The vendor’s project/work plan will be thoroughly reviewed and discussed at the initial implementation kick-off meeting. At that time, the project/work plan and its task lists, timelines and milestones will be approved by both parties. The dates established for completion of each task and phase, and submission of each deliverable in compliance with contractual requirements will form the enforceable service level agreement between the vendor and ISBE.

The vendor is responsible for organizing the review of deliverables with the coordinator at ISBE. A final version of each deliverable must be provided to ISBE by the due date specified on the
finalized project work plan. Final deliverables that meet contractual requirements will be approved by ISBE management. Deliverables that do not meet contractual requirements will be returned to the vendor for revisions until contractual requirements are met. Deliverables submitted after their scheduled draft and/or final version completion dates will be reviewed in a timely manner.

The vendor will be required to formally submit weekly project status reports and other such documentation as specified herein. Each weekly project status report will contain an updated and current task list that reflects the status of on-going tasks, task owners and new tasks added to complete the scope of work. For all submitted project documentation, the vendor is required to use the standard Microsoft® Office 2007 or later version (if adopted by ISBE) product suite for any and all updates of project correspondence, reports, plans, task lists, timelines and deliverables unless ISBE gives written permission to use an alternate product.

It is acceptable to ISBE that during the course of the project, specific phases may overlap.

1.4.1. DELIVERABLES

Phase I-A: Implementation Deliverables
As described herein, the vendor will organize and host a project implementation meeting to be held at ISBE’s Springfield office facility. The vendor is responsible for all travel and accommodation costs associated with this meeting and ISBE will not pay charges related to such expenses. The purpose of the implementation or kick-off meeting is to introduce vendor and state personnel; identify roles and responsibilities (including the designated vendor’s project manager and the ISBE coordinator); review the project plan, task list, timeline, deliverables and other related documentation; and to reach mutual agreement on any proposed changes to the project plan, task list, timeline, deliverables and other related documentation. Deliverables during this phase include:

• **Deliverable 1: The implementation kick-off meeting will occur within 15 work days of the contract’s execution.**
  
  ➢ The kick-off meeting will be held at ISBE’s Springfield office building, at which time specific roles and responsibilities (including ISBE management signature approval) of the parties and teams will be disclosed.
  
  ➢ **Five work days prior to the implementation kick-off meeting,** the vendor will submit project documentation to the ISBE coordinator including, but not limited to:
- A proposed kick-off meeting agenda,
- A list of vendor participants (including the vendor's project manager), their roles in the project and a brief biography of each vendor participant (including endorsements, licensure and certifications earned),
- A proposed schedule for interviews/meetings with ISBE staff,
- A draft of the proposed project/work plan, task lists, milestones and timeline, and deliverables' due dates.

  ✓ ISBE anticipates the project/work plan will include, but not be limited to:
  ▪ Defined project phases,
  ▪ The proposed duration for each task and each project phase,
  ▪ All tasks and objectives,
  ▪ A complete project timeline,
  ▪ A list of dependencies for each phase and each task,
  ▪ An itemization of project milestones and deliverables,
  ▪ Identification of phase and task owners, and
  ▪ The anticipated work approach to complete each task and each phase.

  • **Deliverable 2: Within five work days following the kick-off meeting.** Both ISBE and the vendor will sign off on any changes to the project plan, task list, milestones, timeline and deliverables made by mutual agreement during the kick-off meeting. The vendor will edit and submit the finalized project plan/timeline (including the task list, timeline, milestones and deliverables) to ISBE. The resulting established timelines must contain a completion date for each project phase and a submission date for each deliverable. The mutually agreed upon and signed project plan as described herein will form the enforceable service level agreement between the vendor and ISBE.

    ➢ The vendor will obtain authorized signatures upon completion of the implementation/kick-off project phase.

If the vendor fails to host the required implementation meeting within the required timeframe and/or if the vendor fails to submit the finalized project plan as specified herein, liquidated damages will be assessed per Section 29.3.
Phase I-B: Implementation - Information Gathering Deliverables

Vendor interview and research notes, along with all other documentation, are considered "audit work papers" and are not necessarily deliverables for this project; however, during the course of the project, the notes and documentation must be available to ISBE staff for reference until project completion. Upon conclusion of the project, all project documentation will be delivered to the ISBE coordinator.

As stated herein, ISBE is reliant on electronic infrastructure. There are over 150 applications, network and interconnections to LEAs, schools, universities and nonprofits. This IT Risk Assessment analysis will focus on these key components. During the information gathering phase, key vendor personnel, including the project manager, will be expected to conduct a sufficient number of on-site meetings with ISBE staff to discuss each component in detail. Specific applications for research, review and analysis include, but are not limited to, those identified below.

**Student Information System (SIS) and the Illinois Longitudinal Data System (ILDS)**

Description: Accessible through the ISBE Web Application Security (IWAS) system, SIS is a state-wide student information system linking student outcomes across primary/secondary/post-secondary education and educational agencies that have differing roles and varying access levels. Review and analysis will encompass, but not be limited to:

- A review of trust models for data disclosure;
- Functional testing;
- A review of vulnerabilities that might allow unauthorized data disclosure to attackers, malicious insiders and accidental discovery by authorized users; and
- A review of interconnections to identify weak links or vulnerable data communications channels.

**Teacher Information Systems (Teacher Licensure Information System [ELIS], Employment Information System [EIS])**

Description: Contains Personally Identifiable Information (PII) for educators and administrators, and all records relevant to their certification and licensure history in the State of Illinois. Review and analysis will cover, but not be limited to:

- Minimum data needed to accomplish objectives;
- Frequency of data inventory;
- Security controls for each data category;
- Storage, access and transport; and
- Incident response plan.

**ISBE Web Application Security (IWAS)**

Description: IWAS is the web portal through which school districts and regional offices of education (ROEs) throughout the state access various ISBE applications. As the central point of authentication for dozens of ISBE applications, the vendor assessment will include testing and evaluation to ensure the efficacy of the authentication, authorization and encryption features, as well as session management, data validation and bounds checking, and error handling and logging. Educators throughout the state access the educator licensure application (ELIS) through the IWAS for Educators portal. Review and analysis for these two portals will include, but not be limited to:

- Functional testing;
- A review of vulnerabilities that might allow unauthorized data disclosure to attackers, malicious insiders and accidental discovery by authorized users;
- A review of interconnections to identify weak links or vulnerable data communications channels;
- Black and/or white box testing;
- Source code review; and
- Interface penetration testing.

**Illinois Interactive Report Card (IIRC)**

Description: The IIRC and MyIIRC portal are both hosted at Northern Illinois University (NIU) and ISBE provides data to the IIRC that is used to populate reports on education performance and provide educators access to student performance data. For this externally hosted system, a review of inter-agency agreements, processes and data-transfer mechanisms between sites will be included to assure best industry security practices are in place.

In addition to the specific application named above, the vendor will perform a review and assessment that includes, but is not limited to, the following specific areas of the ISBE infrastructure and network:

- System-wide review of ISBE interconnectivity;
- Physical (infrastructure) security architecture, firewalls and boundaries;
- Proposed virtual network implementation plan;
- File transfer systems for both legacy and newer applications, specifically those applications housing district, administrator, school, faculty, personnel and/or student information subject to the requirements of the Family Educational Rights and Privacy Act (FERPA) and the Illinois School Student Records Act (ISSRA);
- ISBE office automation systems, production and development environments;
- Program/application-level security architecture of the applications itemized above;
- Recorded and live webinars, live videoconferencing and go-to-meeting functionality;
- Third-party oversight processes (projects involving contractors for IT-based projects);
- Incident management processes and incident handling procedures;
- Equipment deployment processes;
- Enterprise-wide review of security plans and existing security policy;
- IT Security and Awareness training program for agency-wide staff; and
- All existing security policies in place.

- **Deliverable 3:** The vendor will submit weekly status reports during the information gathering project phase.
- **Deliverable 4:** The vendor will submit weekly and updated task lists during the information gathering project phase.
- **Deliverable 5:** The vendor will submit a list itemizing the specific infrastructure, application, network and interconnection components for which information was gathered during this project phase.
- **Deliverable 6:** The vendor will obtain authorized signatures upon completion of the information gathering phase.
If vendor fails to submit the required deliverables and/or fails to complete the information gathering project phase as specified in the final project plan timeline, liquidated damages will be assessed per Section 29.3.

**Phase II: Analysis Deliverables**
The vendor will dedicate sufficient time for its qualified and well-experienced security and risk assessment specialists to perform a complete analysis for the IT Risk Assessment. The vendor's analysis will be based on the information gathering phase, including but not limited to, on-site meetings conducted with ISBE personnel, documentation resulting from these on-site interviews and the bullet points contained in section 1.4 *Information Gathering Deliverables*. During this phase, a complete analysis of ISBE systems, policies, practices, controls, environment and applications will be synthesized.

- **Deliverable 7:** The vendor will submit *weekly status reports* during the analysis project phase.
- **Deliverable 8:** The vendor will submit *weekly and updated task lists* during the analysis project phase.
- **Deliverable 9:** The vendor will submit a list itemizing the specific infrastructure, application, network and interconnection components that were analyzed during this project phase.
- **Deliverable 10:** The vendor will obtain *authorized signatures* upon completion of the analysis phase.

If vendor fails to submit the required deliverables and/or fails to complete the analysis phase as specified in the final project plan timeline, liquidated damages will be assessed per Section 29.3.

**Phase III: Reporting Deliverables**
As stated above, the vendor will conduct a sufficient number of meetings with the ISBE coordinator and designated ISBE personnel to relay details of its analysis and explain all findings as presented in the written report. These findings and reports should be focused on each area of IT operations and the gaps between identified vulnerabilities and defined risks in ISBE's current environment, and the recommendations for corrective policies, practices, controls and safeguards that would mitigate exposure to an acceptable,
manageable level. Deliverables include the detailed final analysis report, recommendations for existing security policy revisions along with drafted language for new security policies as may be applicable, a formalized Risk Mitigation Plan and an abridged Executive Summary. The vendor's report analysis and Risk Mitigation Plan will specify the prescribed methodology and standards used in their development.

- **Deliverable 11**: The vendor will submit **weekly status reports** during the reporting phase.
- **Deliverable 12**: The vendor will submit **weekly and updated task lists** during the reporting phase.
- **Deliverable 13**: The vendor will submit a **revised set of reports** delivered to the ISBE coordinator prior to each meeting.
- **Deliverable 14**: By the date specified in the finalized project plan/timeline, the vendor will edit all analysis documentation and submit a finalized, **detailed IT Risk Assessment Analysis Report** to the ISBE project coordinator.

➢ Relative to the **SIS/ILDS system reviews**, the vendor's report will include a specific **statement that ISBE documentation and policies are in place and that SIS/ILDS are in compliance with the relevant requirements of the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g) and the Illinois School Student Records Act (ISSRA) (105 ILCS 10/1 et seq.) regarding the confidentiality of student “education records” as defined in FERPA and “school student records” as defined in ISSRA. If said statement cannot be made, the report will itemize all changes and modifications necessary to assure compliance.

➢ Relative to the **ELIS/EIS system review**, the vendor will provide **specific recommendations** regarding:
  
  o security controls for each data category;
  o storage, access and transport; and
  o a robust incident response plan.

➢ Relative to the **IWAS system application review and analysis**, **recommendations will be included** for all tested elements, including trusted algorithms for encryption and hashing functions.
Relative to the IIRC and other system/application reviews, vendor's report will include recommendations regarding security controls for all data categories and incident response plans, in addition to commentary and recommendations on storage, access and transport.

• **Deliverable 15:** Recommendation for creation of (or procurement of) canned software to deliver an IT Security and Awareness training program to agency-wide staff. The recommended application should provide general information to employees and more advanced training to administrators and be renewable (or ISBE should have the ability to upgrade) to reflect changes in the risk environment and changing best practices. The application should cover, but not be limited to:
  - Common threats,
  - Employee roles and responsibilities,
  - Recognizing and reporting intrusions/breaches,
  - Building an internal security-aware culture,
  - Annual monitoring of employee compliance, and
  - Sources for themed postings, internal emails, newsletters, etc.

• **Deliverable 16:** Recommendation for changes to existing security policies and fully developed new policy language including, but not limited to:
  - Centralized Review and Configuration Management Policy,
  - Dedicated Security Staff Policy,
  - Incident Response Team Policy,
  - System Administrator Security Policy,
  - Audit Log Policy (covering generation/transmission/retention/storage/disposal), and
  - Security Integration as part of the Development Process Policy.

• **Deliverable 17:** By the date specified in the finalized project plan/timeline, the vendor will present the IT Risk Assessment Analysis Report accompanying the Risk Mitigation Plan to the ISBE project coordinator. The Risk Mitigation Plan will include, but not be limited to:
  - Identification of current ISBE policies, practices, controls and safeguards in place and related risk exposure;
Recommendations to maintain or modify current policies, practices, controls and safeguards;

Prioritization of all recommendations for change and justification for the prioritization order;

Disclosure of the criteria used to identify any vulnerabilities and/or weaknesses;

A complete list of identified vulnerabilities and defined risks identified during the analysis described herein;

Baseline security requirements addressing security controls in the areas of computer hardware and software, data and data transport, operations, infrastructure and architecture, administration, management information, peripheral equipment deployment and maintenance, facility communication, personnel, and contingency;

Identification of policies, practices, controls and safeguards in need of revision, and proposed language to assist ISBE in editing and re-writing existing policies, practices, safeguards and controls language for ISBE's potential adoption;

Identification of needed new policies, practices, controls and safeguards and recommended language drafted for new policies, practices, controls and safeguards for ISBE's potential adoption;

Other recommended corrective actions that encompass a set of security baseline essentials that will allow management to make decisions about security-related initiatives;

Recommendations for development or purchase as related to IT, including: hardware, software, architecture, staffing, and incident management and deployment practices;

Recommendations for development or purchase of an IT Security Awareness Training program and any other relevant IT training needs;

Recommendations for key risk/security personnel;

Recommendations to ISBE leadership for the adoption of heightened security measures at the agency-wide level;

Re-engineered flow diagrams, as may be necessary, that document any recommended changes in processes, procedures and controls; and

Other recommendations for adoption of security best practices that safeguard against exposure.
• **Deliverable 18:** By the date and time specified in the finalized project plan and timeline, the vendor will present an electronic copy of the prepared **IT Risk Assessment Executive Summary** to the ISBE project coordinator. (See *Presentation Phase* for details on content.)

• **Deliverable 19:** The vendor will obtain **authorized signatures** upon completion of the reporting phase.

If the vendor fails to submit the required deliverables and/or fails to complete the reporting phase as specified in the finalized project plan timeline, liquidated damages will be assessed per Section 29.3.

**Phase IV: Presentation Deliverables**
The vendor will host a formal presentation at ISBE’s Springfield office that will represent an Executive Summary for the IT Risk Assessment. The ISBE coordinator will assist in establishing the date and facilitating the presence of all essential ISBE personnel. Based on the finalized report(s), the vendor’s presentation will identify recommendations, existing policies, practices, safeguards and controls that need improvement, and will also contain new policies, practices, safeguards and controls recommended as may be needed to hold exposure of operations to a manageable level.

• **Deliverable 20:** The vendor will submit to the ISBE project coordinator a **summary of vendor project activities** (including a finalized task list) related to information gathering and the subsequent review and analysis processes and procedures.

• **Deliverable 21:** The vendor will produce and **host an IT Risk Assessment Executive Summary presentation** (Power Point or other ISBE approved format) to review summaries of finalized report(s) and the Risk Mitigation Plan described herein. As stated above, an electronic copy of the Executive Summary presentation will be submitted to the ISBE coordinator prior to the scheduling of the presentation meeting. The Executive Summary presentation will occur by the date specified in the finalized project plan/timeline.

  ➢ As directed by the ISBE project coordinator, the vendor will present either electronic or hard **copies of the IT Risk Assessment Executive Summary presentation** to ISBE leadership staff at the time of the presentation meeting.
Following the Executive Summary presentation, the vendor will **host a Q&A session**, accompanying or as part of the Executive Summary presentation.

- **Deliverable 22**: The vendor will obtain **authorized signatures** upon completion of the presentation phase.

If the vendor fails to complete this phase and host the Executive Summary presentation by the date specified in the finalized project plan/timeline, liquidated damages will be assessed per Section 29.3.

### 1.4.2. PROPOSED PROJECT TIMELINE

As stated above, the vendor will present a proposed realistic and well-thought out project/work plan with accompanying milestones and timelines. The project/work plan will be reviewed and discussed at the initial implementation kick-off meeting and finalized by a mutual written agreement of both parties. The dates established for completion of milestones and phases, and submission of each deliverable will form the enforceable service level agreement between the vendor and ISBE.

ISBE anticipates that the project will have a duration of no longer than six months.

### 1.5. OFFEROR / STAFF SPECIFICATIONS: STAFF QUALIFICATIONS

ISBE desires vendors with a minimum of five years past experience in performing IT Risk Assessments similar to the goals and tasks outlined herein. Experience in performing IT risk assessments for large municipal/county/state/federal government organizations, especially educational entities, is preferred. To demonstrate the Offeror's expertise and ability to complete the project/work plan, bids should provide descriptions of similar projects completed for other governmental and/or corporate bodies whose projects were of a similar size and scope. ISBE desires vendors with a minimum of 5 years' experience in the development of IT policies, practices, controls and safeguards. Bid submissions should contain an itemization of industry awards and recognition, along with detailed company background and qualifications as they relate specifically to performing IT Risk Assessments and the formulation of IT policies, practices, controls and safeguards. In addition to the staffing plan mentioned above, bids should also identify each staffer's proposed project role.
and a copy of each staffer's resume (including earned endorsements, licensure and certifications).

<table>
<thead>
<tr>
<th>Vendor Qualifications:</th>
<th>Total 300 Points Possible</th>
</tr>
</thead>
<tbody>
<tr>
<td>• (120 PTS) Corporate years of operations/experience and detailed corporate background</td>
<td></td>
</tr>
<tr>
<td>&gt; Vendor should demonstrate its corporate years of experience, specifically related to conducting IT risk assessments for governmental bodies, including educational entities.</td>
<td></td>
</tr>
<tr>
<td>&gt; Vendor should demonstrate its corporate years of experience in formulation and development of IT policies, practices, controls and safeguards.</td>
<td></td>
</tr>
<tr>
<td>&gt; Vendor should list any industry awards and/or recognitions.</td>
<td></td>
</tr>
<tr>
<td>• (90 PTS) Vendor should demonstrate its ability to complete complex projects within a stated time frame.</td>
<td></td>
</tr>
<tr>
<td>• (60 PTS) Project staff roles and responsibilities</td>
<td></td>
</tr>
<tr>
<td>&gt; Vendors should identify each member of the work team and provide their resumes including licenses, endorsements and certifications relevant to the work described in Section 1 of this RFSP.</td>
<td></td>
</tr>
<tr>
<td>&gt; Vendors also should list the major work team roles and associated responsibilities.</td>
<td></td>
</tr>
<tr>
<td>• (30 PTS - 15 PTS for each reference) Vendor should provide professional references from governmental or other corporate bodies whose projects were of similar size and scope, including educational entities. ISBE will select and interview two references using the following questions:</td>
<td></td>
</tr>
<tr>
<td>&gt; Did the vendor meet all due dates for project milestones and deliverables?</td>
<td></td>
</tr>
<tr>
<td>&gt; Was vendor’s project management team cooperative, efficient, and effective in completing all assignments and meeting your expectations?</td>
<td></td>
</tr>
<tr>
<td>&gt; Would you hire this vendor again? Why?</td>
<td></td>
</tr>
</tbody>
</table>

1.6. TRANSPORTATION AND DELIVERY TERMS: N/A

1.7. SUBCONTRACTING

1.7.1. Subcontractors are allowed. For the purposes of this section, subcontractors are those specifically hired to perform all or part of the work covered by the contract. If subcontractors are to be utilized, Offeror must identify subcontractors with an annual value of more than $50,000 and the expected amount of money each will receive under the contract in Attachment FF - Subcontractor Disclosure.
1.7.2. The maximum percentage of the goods or services that are the subject of this offer and the resulting contract that may be subcontracted is N/A.

1.7.3. The Offeror shall notify the State of any additional or substitute subcontractors hired during the term of this contract. If required, Offeror shall provide the State a copy of all such subcontracts within 15 days after execution of this contract or the subcontract, whichever occurs later.

1.7.4. Any subcontracts entered into prior to award of the Contract are done at the Vendor’s and subcontractor’s risk.

1.8. WHERE SERVICES ARE TO BE PERFORMED

1.8.1. Unless otherwise disclosed in this section, all services shall be performed in the United States. This information and the economic impact on Illinois and its residents may be considered in the evaluation. If the Offeror performs the services purchased hereunder in another country in violation of this provision, such action may be deemed by the State as a breach of the contract by Offeror.

1.8.2. Offeror shall disclose the locations where the services required shall be performed and the known or anticipated value of the services to be performed at each location. If the Offeror received additional consideration in the evaluation based on work being performed in the United States, it shall be a breach of contract if the Offeror shifts any such work outside the United States.

1.8.3. Location(s) where services will be performed: Securance Consulting Corporate Office (6922 W. Linebaugh Ave., Ste. 101, Tampa, FL 33625); ISBE Springfield Office; ISBE Chicago Office (Disaster Recovery Center)

1.8.4. Percentage of contract of services performed at these locations: Securance Consulting Corporate Office – 17%; ISBE Springfield Office – 77%; ISBE Chicago Office – 6%

As stated above, the vendor will host the implementation meeting and conduct much of the information gathering phase at ISBE’s Springfield office. It is expected that some of the final analysis and reports may be generated from the vendor’s business location. If the vendor later determines that in the best interest of ISBE project completion, the vendor should spend a greater amount of time at the ISBE Springfield office, a written request should be submitted to the ISBE internal project coordinator for ISBE management approval.

Include Section 1 and any attachments in Packet 1
Proposed Scope

Execute, Analyze, REPORT and Improve
Based on our understanding of the scope of requested services, Securance will execute the following activities:

Phase I-A: Implementation
- Hold a Kick-Off Meeting at ISBE’s Springfield Office Building.
- Submit Deliverable 1 Five Work Days Prior to the Kick-Off Meeting:
  - Meeting agenda;
  - List of project staff and project staff resumes;
  - Proposed meeting I interview schedule; and
  - Proposed project plan.
- Submit Deliverable 2 Within Five Work Days Following the Kick-Off Meeting:
  - Finalized project plan.
  - Obtain authorized signatures upon completion of Phase I-A.

*The kick-off meeting will take place within 15 work days of contract execution.*

Phase I-B: Information Gathering
- Conduct Interviews with Key Personnel:
  - Gain an understanding of network architecture, systems and IT processes.
- Submit Deliverables 3 through 6 (in order):
  - Weekly status reports;
  - Weekly updated task lists;
  - List itemizing the infrastructure, application, network and interconnection components researched during Phase I-B; and
  - Authorized signatures obtained upon completion of Phase I-B.
Proposed Scope

Phase II: Analysis

- Perform an IT Risk Assessment that includes:
  - Security Assessments of Critical Applications:
    - Perform security assessments of critical applications, including:
      - Student Information System (SIS) and the Illinois Longitudinal Data System (ILDS);
      - Teacher Information Systems:
        - Educator Licensure Information System (ELIS);
        - Employment Information System (EIS); and
      - Illinois Interactive Report Card (IIRC).
    - See detailed methodology on page 29.
  - A Security Assessment of ISBE Web Application Security (IWAS):
    - Perform a web application assessment:
      - Unprivileged web application testing (i.e., testing the web application without login information):
        - Identify web applications;
        - Perform an assessment of the hosting server and associated web server’s configuration;
        - Perform unprivileged web application vulnerability testing; and
        - Pending testing and authorization, attempt to modify application’s content.
      - Privileged web application testing (i.e., testing the web application without login information):
        - Identify web applications;
        - Perform an assessment of the hosting server and associated web server’s configuration;
        - Perform privileged web application vulnerability and configuration testing; and
        - Pending testing and authorization, attempt to modify application’s content.
    - See detailed methodology on pages 30 – 31.
  - Perform a Network Architecture Review:
    - Perform a network architecture review.
    - (See detailed methodology on page 32.)
  - Perform Firewall Reviews:
    - Perform firewall reviews.
    - (See detailed methodology on page 33.)
  - Perform a Policies and Procedures Review:
    - Perform a comprehensive review of IT security policies and procedures, including those that govern:
      - Data classification and ownership;
      - Data transmission;
      - Escalation management;
      - Remote access;
      - Virus protection;
      - End use computing;
      - Incident management;
      - Wireless services;
      - Monitoring and logging;
      - IDS/IPS; and
      - Configuration management.
    - (See detailed methodology on page 34.)
Proposed Scope

Phase II: Analysis (continued)

- Formulate Recommendations Regarding the IT Security Awareness Training Program.
  - Formulate recommendations regarding the use of software to deliver an effective IT security awareness training program.
- Submit Deliverables 7 through 10 (in order):
  - Weekly status reports;
  - Weekly updated task lists;
  - List itemizing the infrastructure, application, network and interconnection components analysed during Phase II; and
  - Authorized signatures obtained upon completion of Phase II.

Phase III: Reporting

- Submit Deliverables 11 through 19 (in order):
  - Weekly status reports;
  - Weekly updated task lists;
  - Revised set of reports delivered to ISBE Project Coordinator prior to each meeting;
  - IT Risk Assessment Report;
  - Recommendations regarding the use of canned software to deliver an IT Security Awareness Training Program to staff;
  - Recommendations for changes to existing IT security policies and procedures and drafted language for new policies;
  - Risk Mitigation Plan;
  - Electronic copy of Executive Summary; and
  - Authorized signatures obtained upon completion of Phase III.

Phase IV: Presentation

- Submit Deliverable 20:
  - Summary of project activities.
- Conduct an Executive Summary presentation (Deliverable 21):
  - Review final report and Risk Mitigation Plan; and
  - Host a question-and-answer session.
- Submit Deliverable 22:
  - Authorized signatures obtained upon completion of Phase IV.
Approach and Methodology

IT Audit Approach and Methodology

Our audit approach is unlike that of any other professional services or accounting firm. We focus on technology risk as it translates into business risk.

Our approach will focus on continuous assessment of ISBE’s IT controls. As we begin the audit process, we will work closely with Internal Audit Management to better understand key technology issues and changes in the organization’s IT environment.

We will leverage available resources in your IT and Internal Audit Departments – teaming to eliminate unnecessary duplication of effort, to enhance quality and to maximize cost effectiveness. Securance Consulting’s continuous assessment of these factors will result in discussions with Management to determine what procedures should be performed during the audit, who should perform them and when they should be performed.

As a result, we will strategically focus our efforts on areas of high technology risk. Ultimately, our process will deliver assurance. Our audit results are objective. Through continuous communication throughout the process, we deliver a real-time view of technology risk, providing early warnings and no surprises.
Approach and Methodology

Initial planning meeting:
- Team introductions
- Methodology discussion & clarification
- Project scope analysis
- Project timeline definition
- Risk matrix completion
- Audit guidelines to be followed

Memo defines the project audit strategy and addresses the following areas:
- Planning meeting summary
- Client background
- Audit scope
- Technology under review
- Technology structure (i.e., 3-tier, 2-tier, etc.)
- IT control environment & internal control structure

Technical memo captures a summary of the IT environment, including:
- Applications
- Business processes being supported
- Host names & addresses
- Host platforms
- Application development method
- Access control solutions
- Management control solutions
- Telecommunication topology

Internal control documentation captures a summary of the current state of control throughout the IT environment, including:
- IT strategic planning in support of company objectives
- System development and program change management
- Business continuity
- Disaster recovery
- Remote access management
- Policies & procedures
- Logical & physical access
- Network controls
- System monitoring solutions

Detailed listing of the procedures to be performed to ensure accurate value-added results:
- Team introductions
- Reviewed & approved by client
- Planning procedures
- Data & system access procedures
- Platform interrogation
- Technology-specific review steps
- Change procedures
- Test of identified controls
- Other technology issues identified
- Wrap-up procedures

Our consultants use their experience, technology skill and a variety of commercial and proprietary tools to perform the procedures outlined in the review program.

Our process includes a structured set of eWorkpapers and an independent review to support our findings.

Our consultants use the review program as a guide and perform additional procedures, if necessary.

The final project deliverable is an easy-read executive summary.

This report includes:
- Applications
- Brief background of the project
- Executive summary of findings and recommendations
- Technical summary of findings and recommendations
- Value scorecard - listing of business value provided by the engagement
Approach and Methodology

CoBIT Objectives
IT controls should consider the overall governance framework to support the quality and integrity of information.

Plan & Organize
PO1 Define a Strategic Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organization & Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims & Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess & Manage IT Risks

Deliver & Support
DS1 Define & Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance & Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify & Allocate Costs
DS7 Educate & Train Users
DS8 Manage Service Desk & Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations

Acquire & Implement
AI1 Identify Automated Solutions
AI2 Acquire & Maintain Application Software
AI3 Acquire & Maintain Technology Infrastructure
AI4 Enable Operation & Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install & Accredit Solutions & Changes

Monitor & Evaluate
ME1 Monitor & Evaluate IT Performance
ME2 Monitor & Evaluate Internal Control
ME3 Ensure Compliance with External Requirements
ME4 Provide IT Governance
Approach and Methodology

Application Security Assessments
The methodology that Securance uses to assess application security for internally developed applications is flexible. It is designed to follow the system development life cycle (SDLC) methodology (e.g., waterfall, agile, JAD, etc.) used to develop the application. It also takes into account the project management methodology (PMM). Our procedures include:
- Interviewing lead developers to understand the application's architecture.
- Gaining an understanding of the application's functionality.
- Understanding the SDLC and PMM in place.
- Reviewing the application's design, architecture and environment documentation.
- Performing tests and audit procedures to ensure that development adheres to the SDLC and PMM.
- Performing tests and audit procedures to ensure that development phases are consistent with design documentation.
- Assessing the level of Management review and sign-off on designs, development and all forms of testing.
- Assessing compliance with the organization's guidelines regarding application controls – including input and output controls, validation checks and edit controls.
- Documenting and performing negative and positive tests of all technical controls.

In addition, each application will be assessed using our General Computer Controls Review (GC²R) methodology. This methodology follows the CoBIT Framework and includes an assessment of the design and operating effectiveness of the following IT Processes:
- IT governance and management (IT policies and procedures);
- Backup and recovery;
- Change and patch management;
- Incident management;
- Job scheduling;
- System development life cycle methodologies (SDLC);
- Software license compliance (if applicable); and
- Source control (if applicable).
Approach and Methodology

Web Application Security Assessment
The Securance web-application testing methodology includes looking for vulnerabilities at various layers and testing the overall security of web applications. Securance Consulting will perform an in-depth analysis of publicly available web servers, concentrating on security-related issues including, but not limited to:

- Cross Site Scripting (XSS)
- Malicious File Execution
- Insecure Direct Object Reference
- Information Leakage and Improper Error Handling
- SQL Injection
- CRLF Injection
- Remote Execution
- Directory I File Traversal
- PHP File Include
- Parameter Deletion
- Special Parameter Addition
- Boolean Parameter Tampering
- Broken Authentication and Session Management
- Buffer Overflow
- Format String
- Integer Overflow
- Information Exposure
- Generic HTTP Attacks
- Microsoft CGI Attacks
- CGI Attacks
- Microsoft IIS Attacks
- Common HTTP Device Attacks
- Cross Site Request Forgery (CSRF)
- Failure to Restrict URL Access
- Insecure Communications
- Insecure Cryptographic Storage
- Blind SQL Injection
- Injection Flaws

In addition to the procedures described above, the Securance web-application security testing methodology includes:

OS Level Assessment
- If access is to the operating system is obtained or provided, we perform a detailed security review of the operating system configuration. These procedures are performed against all servers that comprise the web application infrastructure.

Database Assessment
- In addition to the operating system-level procedures, we perform a comprehensive security analysis against the portal’s backend database. Initial attempts are made to access the database without credentials. Pending success, we perform a database-specific vulnerability scan using commercial tools (e.g., Application Detective or SecureSphere).

Web Login Assessment
- Our methodology includes assessing the web application by logging into the application and testing for various vulnerabilities. Our process will uncover hidden input fields; test input parameters; crawl the portal and identify exploratory features; attempt to discover sensitive and private information; uncover common software writing errors; identify common injection vulnerabilities that may allow malicious code execution; and assess error handling that may expose the application.
Source Code Review (if applicable)
The Security source code review methodology begins with gaining a detailed understanding of the application's architecture. This is achieved through interviews with the application owner, senior developer and business owner. The following additional steps aid in understanding the application prior to performing an automated source code review:

- Gaining an understanding of the system development life cycle (SDLC) methodology that was used to guide development;
- Gaining an understanding of the development and coding standards in place;
- Reviewing all available requirements, design, UI and technical documentation;
- Performing a structured walkthrough of the source code; and
- Reviewing all available project plans, tracking systems and testing documentation.

Upon completing the above tasks, we then assess the source code using an automated source code analyzer. This process is useful to complete the following:

- Identify calls to insecure library functions;
- Detect type confusion;
- Detect memory errors;
- Identify vulnerabilities in sequence of operations;
- Perform data flow and loop analyses; and
- Identify potential buffer overflows.
Approach and Methodology

Network Architecture Review
The Securance methodology for assessing the design and architecture of a core network is to ensure the network is designed to provide users with as much bandwidth as possible, as often as possible. In our opinion, the best network design is the one that meets the needs of its users. There is no one “correct” switched design; there are only proven design principles that should be incorporated where possible. Designs can differ based on a number of real-world factors, including budgets, available existing hardware, application requirements and implementation timelines. The Securance approach is to understand the network and user requirements and weigh the pros and cons of each design principle against the overall goals for the design.

Current practices recommend a Layer 3/4 switched network. Our analysis includes a review of all 3 layers and the configuration sets (i.e., switching and routing) at each layer. The other areas we analyze include:

- Routers should be intelligently and securely configured. They are another security skin and should be leveraged.
- We review all unused ports to ensure they are disabled.
- Routers should be used to bin generic classes of undesired traffic before they hit any firewall.
- The company uses Private IPs on the internal and DMZ networks.
- The external router bins Private IP addresses, while the internal core bins any connections that have an Internet IP as the originating address.
- The external router also bins any unknown protocols not provisioned in the DMZs.
- All three parties are handled with IPSEC to the remote location and terminated in a DMZ.
- A choke VLAN exists which enforces an inspection point for IDS and IPS systems.
- The servers in the data center are protected by a separate firewall.
- All business unit servers are in separate VLANs.
- External connections are facilitated via reverse proxies hosted in a DMZ.
- Email is relayed via a bridge head in a DMZ. Use is made of mail scrubbing services.
- DNS is properly and securely configured.
- Workstations are separated into functional business unit bases. This stops any worms and Trojans in its tracks and prevents information leakage.
- On the inside networks, all route distribution is authenticated, especially routes between the firewalls and the core.
- A separate network management VLAN exists, accessed off the core and protected by ACLs.
- The management VLAN should contain jump servers which are the designated points to access all network device and firewall consoles.
- Do not publish intranet on port 80; rather, use port 8080 to 8090. This will assist with controlling web traffic.
Firewall Review
The following are included in our firewall analysis:
- Interview Firewall Administrator(s).
- Review configuration manually.
- Review rule set line by line.
- Identify problem rules.
- Identify redundant rules.
- Identify circular rules.
- Perform a vulnerability scan of device.
- Assess firmware version.
- Ensure compliance with change management.
- Assess access controls.
- Review logs manually.
- Perform automated review of logs using a commercial firewall analyzer:
  - Analyze traffic patterns;
  - Identify potential virus and hack attempts; and
  - Recommend potential rules to improve security.
- Assess use of insecure protocols.
Approach and Methodology

Policies and Procedures Review

The Securance methodology for assessing IT system security policies and procedures is comprehensive and addresses all components of IT security. These components include:

- Data classification and ownership
- Data transmission
- Escalation management
- Remote access
- Virus protection
- Firewall security
- End user computing
- Incident management
- Wireless services
- Monitoring and logging
- IDS / IPS
- Configuration management

In addition to assessing the included components, we perform a comparative analysis against requested frameworks, including ISO, ITIL, CoBIT, NIST and other governing standards. We define a policy as Management’s intentions relative to mitigating a risk. Policies should be supported by detailed procedures that provide guidance to IT engineers and administrators regarding the implementation of the policy.

Our assessment is comprehensive and will likely uncover components and risks not currently being addressed.
Approach and Methodology

Audit Program
Each project we undertake will follow this standard methodology. While we are flexible in modifying our approach and methodology...we do so only in the best interest of our clients and their internal control initiatives.

Project-Specific Risk Analysis
- We begin by selecting the most comprehensive audit program.
- We adjust the audit program based on client-specific risks we learn about during an initial interview process with our client’s Business Process Owner and IT professionals.

Joint Development of Audit | Review Program
- Draft a risk-based audit program and present to client for review.
- Make modifications as deemed necessary by Management.

Execution of Audit Program
- Present a client assistance request list to minimize disruption to staff.
- Schedule on-site interviews and evidence gathering.
- Conduct on-site activities.
- Analyze the results and probe further as deemed necessary.
- Review preliminary findings with Management to confirm results.

Audit Techniques
Our audit techniques are as follows:
- Interviews of appropriate staff;
- Online review of configuration settings;
- Review of hardcopy documentation;
- Positive and negative configuration settings test;
- Sample testing of in-scope processes;
- Utilization of computer auditing techniques for data analysis; and
- Use of software tools to support technical audits and reduce manual efforts.

Software and Computer Tools
Select software and computer tools utilized as deemed necessary include:
- ACL and Monarch - a data extraction and analysis tool;
- Log Reader - an event viewer and application log viewing tool;
- MS Excel;
- Nessus - an open-source vulnerability scanner;
- Sefchek - a scripting tool used to create scripts to extract configuration data from operating systems;
- Firewall Analyzer - a tool for analyzing firewall rule sets and configurations;
- Phonesweep - a package used to identify open modems;
- Web Scanner - a vulnerability scanner specifically designed to assess web applications; and
- Application Scanner - select application scanners.
Approach and Methodology

Documentation Standards
The following section describes our policy and practices with respect to meetings, interviews, and workpaper documentation.

Entrance I Kick-off Conference
- Each of our meetings is supported by an agenda.
- The entrance conference is designed to accomplish the following tasks:
  - Introduce our team to the auditee;
  - Discuss the audit scope, objectives and plan;
  - Review the client assistance request listing to determine if there are any questions;
  - Obtain an understanding of our client’s working environment and other logistics;
  - Define specific milestones and our client’s preferred communication method; and
  - Answer any questions our client may have about the process.

Fieldwork Interviews
- All fieldwork interviews with ISBE personnel will be scheduled in advance and at a convenient time for the interviewee.
- All interviews will be limited to durations of 30 - 45 minutes. If additional time is necessary, a subsequent interview will be scheduled. This is our attempt to minimize disruption ISBE staff members’ workloads.

Findings Documentation
- All potential findings will be documented on an “issue tracker document.” This document is used to ensure that a potential issue is properly documented and associated with adequate evidence to support a finding.
- All findings that are an immediate risk to the organization are immediately brought to the attention of Internal Audit Management and the responsible remediation person or team.

Periodic Reporting
- Depending on the size of a project, we issue weekly or bi-weekly status reports. These reports are designed to capture and communicate the following information about an ongoing project:
  - Budget to actual hours and projected hours to complete project;
  - Project issues or risk that may hinder project completion;
  - Change control items (typically only applicable if the scope changes);
  - Project milestone status;
  - Upcoming activities; and
  - Summary of any potential findings.

Exit Conference
- The exit conference is designed to accomplish the following tasks:
  - Thank our client for providing assistance and support;
  - Review the audit scope, objectives and findings;
  - Potentially present a draft report;
  - Obtain information from our client about report presentation and tone; and
  - Define a timeline for final report review, Management responses and final report delivery.
Regular breaks intentionally.

Try a new activity next time.
Project Management

Each project we undertake will follow this standard accountability model.

**Engagement Manager**
- Ensure the appropriate team is assembled for each project.
- Ensure engagement is performed in a timely way and without any issues.
- Resolve any issues that may arise.
- Deliver and review project reports.

**Senior IT Audit I Security Consultants**
- Draft detailed security procedures.
- Lead the execution of the procedures.
- Prepare workpapers that meet the reperformance standard.
- Identify vulnerabilities and exposures.
- Prepare periodic status reports and review with ISBE's Project Coordinator.

**ISBE's Project Coordinator**
- Coordinate meetings between Securance and ISBE staff.
- Join project interview meetings as considered necessary or desired.
- Review periodic status reports and discuss any concerns with Engagement Manager.
- Provide Securance with guidance relative to ISBE’s mode of operations.
- Review vulnerabilities to obtain a clear understanding of the risks and recommendations.

**Status Reports**
- Depending on the size of a project, we issue weekly or biweekly status reports. These reports are designed to capture and communicate the following information about an on-going project:
  - Budget to actual hours and projected hours to complete project;
  - Project issues or risks that may hinder project completion;
  - Change control items (typically only applicable if the scope changes);
  - Project milestone status;
  - Upcoming activities; and
  - Summary of any potential findings.

*For your reference, we provide a sample status report in Appendix A.*
Information Sharing Security

Safeguards to Protect ISBE’s IT Assets, Including eCommunications

- All Securance Consultants will adhere to a Confidentiality Agreement.

- All Securance Consultants will perform their activities on a Company-issued workstation. The workstation will be configured using whole disk encryption; local firewalls will be enabled; and the anti-virus solution will be current.

- This full-disk encryption software will protect data from unauthorized access, providing strong security for intellectual property, customer and partner data.

- It will often be essential that sensitive information be shared between Securance and ISBE. In these situations, our team will adhere to the following standards:
  - Any sensitive information shared via email must be encrypted.
  - Any reports containing sensitive information must be encrypted and password protected.
  - All passwords used will meet or exceed standard complex password standards.
  - Any passwords that need to be communicated will be communicated via telephone or under separate email cover.

- Any hardcopy documents containing sensitive information will be shredded at the completion of the engagement.

- Engagement information will be shared only with the Engagement Team.

- At the conclusion of the engagement, all electronic data will be permanently deleted from all Consultants’ workstations. All engagement workpapers will be digitized, encrypted and stored on a secure file server. ISBE’s Project Coordinator may direct Securance to destroy all workpapers after an electronic copy has been delivered to the designated personnel.

Workpaper Security Standards

- All working papers are maintained electronically on our secured drive for a period of three years.

- All data on the Securance network is regularly backed up, archived and securely stored according to best practice standards.

- All working papers obtained from clients are considered confidential and treated as such. Securance does not provide any working papers to any third parties without explicit written permission from the client.

- Any data obtained for the performance of the review that is classified as “sensitive” is either reviewed on site or disposed of via best practice standards at the completion of the review; Securance does not retain sensitive client information.

- Upon engagement, Securance will also discuss any further data retention standards required by our clients.
Information Sharing Security

Procedures to Ensure No Disruption to IT Systems

- All vulnerability assessments and penetration testing will be performed after normal business hours or at a
time requested by ISBE's IT personnel.

- All vulnerability assessments and penetration testing will be performed using a policy that ensures no
disruption to the network. If more aggressive scanning procedures need to be performed, they will
only be performed after we obtain explicit approval from ISBE's Project Coordinator.

- All procedures with the potential to be disruptive will be performed using manual techniques and at a
guarded pace. During the performance of these procedures, IT Management will be asked to monitor
network and system performance and to notify Securance Consultants if performance becomes
unacceptable. In the unlikely event of network or system disruption, the active procedures will be
terminated.

Quality Assurance Process

All projects are led by Senior IT Security Consultants with a minimum of 14 years' experience. Their work is
reviewed by the Engagement Manager, and the final product is reviewed by an executive independent of the
project. Additionally, our service level commitment to our clients is as follows:

- Our work product will meet or exceed the requirements of our client's internal standards.

- We ask you to measure our quality based on the comprehensiveness and quality of our reports.

- We ask our clients to complete a Satisfaction Survey.

Independence Assurance Process

Securance Consulting adheres to the principle guidelines outlined in the Institute of Internal Audit Practice
 Standards. Our Management Team ensures that the firm maintains Independence and Objectivity on each project.
Our staff is required to maintain select certifications; this requirement ensures Independence, Proficiency and Due
Care.
Related Experience

Organizations that have trusted Securance Consulting to perform similar professional services include:

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary of Scope</th>
<th>Client Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT General Controls Review</td>
<td>Securance performed an IT general controls review for the Teachers’ Retirement System of the State of Illinois. The scope of the review included: continuous service; IT risk assessment; change control; database controls; security administration; security and controls of confidential electronic information; LAN</td>
<td>Teachers’ Retirement System of the State of Illinois</td>
</tr>
<tr>
<td>Information Security Risk Assessment</td>
<td>The City of Milwaukee contracted with Securance in 2012 to perform an IT risk assessment over critical applications, database technologies and server technologies belonging to several government divisions. The project scope included an assessment of all IT processes, an assessment of IT governance and fact-based testing of select IT processes. Securance also performed vulnerability assessment services for the City in 2011.</td>
<td>City of Milwaukee, WI</td>
</tr>
<tr>
<td>System Security Audits - IT Risk Assessment</td>
<td>Securance performed an IT risk assessment and an IT Risk Assessment for the Colorado Public Employees’ Retirement Association in April and October of 2010 respectively. The system security audit included database vulnerability assessments, multiple security assessments of IT general controls, IT scope technologies and the IT risk assessment concluded with the development of a multi-year qualified</td>
<td>Colorado Public Employees’ Retirement Association</td>
</tr>
<tr>
<td>Application Security Audit</td>
<td>Securance performed IT audits for Frederick County while under contract from August 2009 through June 2011. In 2011, Securance conducted a security assessment of Frederick Community College’s PeopleSoft financial application. The scope of work included testing general computer and application controls and performing a vulnerability assessment over the database supporting the application.</td>
<td>Frederick County, MD</td>
</tr>
</tbody>
</table>
## Related Experience

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary of Scope</th>
<th>Client Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Compliance Review &amp; Application Controls Assessment</td>
<td>The University of Kentucky engaged Securance to perform an assessment of compliance with HIPAA security rules for the Sunrise Clinical Manager (SCM) application system and associated databases. The project scope also included a high-level assessment of general controls for the SCM application.</td>
<td>University of Kentucky</td>
</tr>
<tr>
<td>IT General Control Audit Assessment</td>
<td>Houston Community College contracted with Securance to perform an IT audit in 2015. The objective was to ensure that the college’s general controls were adequate, effective and working as intended across all IT systems, networks and telecommunication environments. Project items included reviews of change request management, policies and procedures, and testing, including physical access control and use provisioning processes. A review of disaster recovery, physical security in data centers, incident response, and incident response incident response.</td>
<td>Houston Community College</td>
</tr>
<tr>
<td>IT Risk Assessment</td>
<td>Securance has been a partner of Louisville – Jefferson County Metro Government (LJCMG) since 2004 and has performed numerous IT services for the organization, including vulnerability assessments and penetration testing, risk assessments and audit services (including application and database reviews). In December 2013, Securance performed an IT risk assessment of the auditable technologies and processes deployed to protect LJCMG’s IT assets. The objectives were to assess the IT systems that store, process and transmit organizational information, and to enable Management to make well-informed decisions regarding the implementation of risk management strategies.</td>
<td>Louisville – Jefferson County Metro Government</td>
</tr>
<tr>
<td>IT Security and General Controls Assessment</td>
<td>Securance performed an IT security and general controls assessment for the City of Bowling Green. The objectives were to identify the organization’s technology-specific vulnerabilities and to assess the general controls. The project’s scope included an assessment of the Internet and external network protocol (IP network), an audit assessment of the IT’s risk, and a review of selected processes.</td>
<td>City of Bowling Green, KY</td>
</tr>
<tr>
<td>IT Security Assessment</td>
<td>Securance performed an IT security assessment for the Orange County Sanitation District. Project items included: an external network vulnerability assessment and penetration test; an on-site internal network security test; a wireless network security assessment; war-dialing; a physical security assessment; and a comprehensive review of IT policies and procedures.</td>
<td>Orange County Sanitation District</td>
</tr>
<tr>
<td>System Security Audit &amp; IT Risk Assessment</td>
<td>Securance performed a security assessment for the Housing Authority of the City of San Buenaventura. The services assessed included: internal and external network security; network security applications and services; server configurations; network and DMZ architecture; incident response; procedures; document management policies; change management procedures; and ISM, NIST, NIST, and organizational structure. Securance also performed staff augmentation services for the HA since 2015.</td>
<td>Housing Authority of the City of San Buenaventura</td>
</tr>
</tbody>
</table>
Timeline and Deliverables

Proposed Project Timeline

On the following pages, we provide a detailed project plan based on our understanding of the scope of services requested by ISBE. The Gantt charts outline each step of our process and designate important milestones throughout the engagement. The staffing charts include itemized tasks and deliverables, task owners and detailed descriptions of the tasks and the task owners' responsibilities.

The project start dates listed in the project plan are intended to show the flow of a project and not the actual project start date. We are flexible in determining the start date of this project and would like to work with the assigned Project Coordinator to determine the start date that works best for ISBE.
<table>
<thead>
<tr>
<th>#</th>
<th>Time</th>
<th>Expected Start</th>
<th>Expected End</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>5/5/14</td>
<td>4/4/14</td>
<td>SBE Proposed Project Plan - Phase 1</td>
</tr>
<tr>
<td>1</td>
<td>Phase I-A: Implementation</td>
<td>5/5/14</td>
<td>1/20/14</td>
<td>Phased Implementation</td>
</tr>
<tr>
<td>2</td>
<td>Deliverable 1</td>
<td>3/5/14</td>
<td>3/10/14</td>
<td>Deliverable 1</td>
</tr>
<tr>
<td>3</td>
<td>Prepare Kick-Off Meeting Agenda, Staff List and Resumes, Proposed Meeting and Interview Schedule, and Proposed Project Plan</td>
<td>3/5/14</td>
<td>1/7/14</td>
<td>Prepare Kick-Off Meeting Agenda, Staff List and Resumes, Proposed Meeting and Interview Schedule, and Proposed Project Plan</td>
</tr>
<tr>
<td>4</td>
<td>Submit Deliverable 1.</td>
<td>5/10/14</td>
<td>1/10/14</td>
<td>Science Deliverable 1</td>
</tr>
<tr>
<td>5</td>
<td>Kick-Off Meeting</td>
<td>3/17/14</td>
<td>3/17/14</td>
<td>Kick-Off Meeting</td>
</tr>
<tr>
<td>7</td>
<td>Deliverable 2</td>
<td>3/18/14</td>
<td>3/19/14</td>
<td>Deliverable 2</td>
</tr>
<tr>
<td>8</td>
<td>Prepare Finalized Project Plan and Obtain Authorized Signatures.</td>
<td>3/18/14</td>
<td>1/18/14</td>
<td>Prepare Finalized Project Plan and Obtain Authorized Signatures.</td>
</tr>
<tr>
<td>9</td>
<td>Submit Deliverable 2.</td>
<td>3/19/14</td>
<td>3/19/14</td>
<td>Science Deliverable 2</td>
</tr>
<tr>
<td>11</td>
<td>Interviews with Key Personnel</td>
<td>3/24/14</td>
<td>3/31/14</td>
<td>Interviews with Key Personnel</td>
</tr>
<tr>
<td>12</td>
<td>Conduct Interviews with SBE IT Personnel.</td>
<td>3/24/14</td>
<td>3/29/14</td>
<td>Conduct Interviews with SBE IT Personnel.</td>
</tr>
<tr>
<td>16</td>
<td>Deliverable 5</td>
<td>3/31/14</td>
<td>4/1/14</td>
<td>Deliverable 5</td>
</tr>
<tr>
<td>17</td>
<td>Prepare Uninterrupted Infrastructure, Application, Network and Interconnection Components Resistant During Phase I-B.</td>
<td>3/31/14</td>
<td>3/2/14</td>
<td>Prepare Uninterrupted Infrastructure, Application, Network and Interconnection Components Resistant During Phase I-B.</td>
</tr>
<tr>
<td>18</td>
<td>Submit Deliverable 5.</td>
<td>4/1/14</td>
<td>4/1/14</td>
<td>Submit Deliverable 5</td>
</tr>
<tr>
<td>Deliverable</td>
<td>Description</td>
<td>Start Date</td>
<td>End Date</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Phase III: Reporting</td>
<td>6/3/14</td>
<td>6/30/14</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Draft Initial Report</td>
<td>6/3/14</td>
<td>6/30/14</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Deliverable 1: Submit Weekly Status Report</td>
<td>6/3/14</td>
<td>6/30/14</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Deliverable 2: Submit Weekly Status Report</td>
<td>6/3/14</td>
<td>6/30/14</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Review Draft Reports</td>
<td>6/3/14</td>
<td>6/30/14</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Review Reports</td>
<td>6/10/14</td>
<td>6/10/14</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Deliverable 3: Submit Revised Reports before Meeting with Project Coordinator</td>
<td>6/11/14</td>
<td>6/11/14</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Review Reports</td>
<td>6/11/14</td>
<td>6/11/14</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Deliverable 3: Submit Revised Reports before Meeting with Project Coordinator</td>
<td>6/12/14</td>
<td>6/12/14</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Prepare Final Reports</td>
<td>6/12/14</td>
<td>6/12/14</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Deliverable 11: Submit Weekly Status Report</td>
<td>6/12/14</td>
<td>6/12/14</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Deliverable 12: Submit Weekly Status Report</td>
<td>6/12/14</td>
<td>6/12/14</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Deliverable 17: Submit Final Risk Mitigation Plan</td>
<td>6/27/14</td>
<td>6/27/14</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Deliverable 18: Submit Electronic Copy of Executive Summary</td>
<td>6/27/14</td>
<td>6/27/14</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Deliverable 19: Obtain Authorized Signatures upon Completion of Phase III</td>
<td>6/30/14</td>
<td>6/30/14</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Phase IV: Presentation</td>
<td>7/2/14</td>
<td>7/2/14</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Deliverable 20: Final Summary of Project Activities</td>
<td>7/2/14</td>
<td>7/2/14</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Deliverable 21: Conduct Executive Summary Presentation</td>
<td>7/2/14</td>
<td>7/2/14</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Deliverable 22: Obtain Authorized Signatures upon Completion of Phase IV</td>
<td>7/2/14</td>
<td>7/2/14</td>
<td></td>
</tr>
</tbody>
</table>
Project Timeline

Staffing Plan

Summary of Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Role Responsibilities</th>
<th>Assigned Staff</th>
<th>Estimated Start Date</th>
<th>Phase(s) (I-IV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engagement Manager</td>
<td>• Serve as initial contact for ISBE Management Team.</td>
<td>Paul Ashe</td>
<td>March 5, 2014</td>
<td>I, II, III and IV</td>
</tr>
<tr>
<td></td>
<td>• Ensure that engagement is performed in a timely manner; resolve any issues that arise.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Deliver and review project reports.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior IT Audit</td>
<td>• Draft detailed security assessment plan and lead plan execution.</td>
<td>Chris Bong</td>
<td>March 5, 2014</td>
<td>II, III and IV</td>
</tr>
<tr>
<td>I Security</td>
<td>• Prepare workpapers that meet reperformance standard.</td>
<td>James McDonald</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultant</td>
<td>• Identify vulnerabilities and risks.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Prepare weekly status reports and review with ISBE Project Coordinator.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Meet with Engagement Manager and project team.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Draft security reports.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Phase I-A: Implementation

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Task Owner</th>
<th>Other Staff Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliverable 1</td>
<td>• Five work days prior to kick-off meeting, submit meeting agenda, staff list and resumes, proposed meeting I interview schedule and proposed project plan.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Kick-Off Meeting</td>
<td>• Hold kick-off meeting at ISBE – Spring Hill Office.</td>
<td>Security Engagement Manager</td>
<td>Senior IT Audit Security Consultant</td>
</tr>
<tr>
<td>Deliverable 2</td>
<td>• Within five work days following kick-off meeting, submit finalized project plan.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Phase I-B: Information Gathering

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Task Owner</th>
<th>Other Staff Required</th>
</tr>
</thead>
</table>
| Interviews with Key Personnel | • Conduct interviews with ISBE personnel.  
                                  • Gain an understanding of ISBE network architecture, systems and IT processes. | Securance Project Team      | ISBE IT Personnel    |
| Deliverable 3                 | Submit weekly task list analyses                                             | Securance Engagement Manager|                      |
| Deliverable 4                 | Submit weekly updated task lists                                             | Securance Engagement Manager| N/A                  |
| Deliverable 5                 | Upon completion of phase 3, obtain authorized signatures in application, networking, and interconnection components processed. | ISBE IT Personnel           |                      |
| Deliverable 6                 | Obtain authorized signatures upon conclusion of Phase 1-B                    | Securance Engagement Manager| N/A                  |
## Project Timeline

### Phase II: Analysis

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Task Owner</th>
<th>Other Staff Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security Assessments</td>
<td>• Perform security assessments of critical applications, including SIS and ILDS, Teacher Information Systems (ELIS and EIS) and IIRC.</td>
<td>Security Project Team</td>
<td>N/A</td>
</tr>
<tr>
<td>Web Application Assessment</td>
<td>• Assess IWAS, perform on-premise, and cloud-based web application assessments.</td>
<td>Security Project Team</td>
<td>N/A</td>
</tr>
<tr>
<td>Network Architecture Review</td>
<td>• Assess network architecture at ISBE Springfield office.</td>
<td>Security Project Team</td>
<td>N/A</td>
</tr>
<tr>
<td>Firewall Configuration Reviews</td>
<td>• Assess firewall configurations at ISBE Springfield office.</td>
<td>Security Project Team</td>
<td>N/A</td>
</tr>
<tr>
<td>IT Security Policies and Procedures Review</td>
<td>• Assess adequacy and effectiveness of existing security policies and procedures.</td>
<td>Security Project Team</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 7</td>
<td>• Submit weekly status reports.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 8</td>
<td>• Submit weekly updated reports.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 9</td>
<td>• Upon conclusion of Phase II, submit list itemizing infrastructure, application, network and interconnection components assessed.</td>
<td>Security Project Team</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 10</td>
<td>Obtain authority clearance for component of Phase II.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Project Timeline

### Phase III: Reporting

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Task Owner</th>
<th>Other Staff Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliverable 11</td>
<td>• Submit weekly status reports</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 12</td>
<td>• Submit weekly updated status reports</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 13</td>
<td>• Deliver revised reports to ISBE Project Coordinator prior to each meeting.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 14</td>
<td>• Submit finalized IT Risk Assessment report</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 15</td>
<td>• Submit final recommendations regarding the use of canned software to deliver IT Security Awareness Training Program to staff.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 16</td>
<td>• Submit final recommendations regarding changes to existing IT security policies and procedures.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 17</td>
<td>• Submit final Risk Mitigation Plan.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 18</td>
<td>• Submit electronic copy of Executive Summary.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 19</td>
<td>• Obtain authorized signatures upon completion of Phase III.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Phase IV: Presentation

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Task Owner</th>
<th>Other Staff Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliverable 20</td>
<td>• Submit final summary of project activities.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 21</td>
<td>• Conduct Executive Summary Presentation.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
<tr>
<td>Deliverable 22</td>
<td>• Obtain authorized signatures upon conclusion of Phase IV.</td>
<td>Security Engagement Manager</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Sample Deliverables

Sample Reports

We provide two (2) sample reports for your review: sample weekly status report in Appendix A and a sample IT risk assessment report in Packet 3, Tab 3. Our methodology is comprehensive and will meet the needs of your organization. Please note that the sample IT risk assessment report is marked "Confidential." We kindly request it be treated as confidential material.
Offeror Qualifications

Securance Consulting - Success Built on Results

Securance Consulting is a professional services firm dedicated to IT security, internal audit risk consulting and compliance. In a decade of rapid and substantial growth, Securance Consulting has found success through the power of a simple idea: deliver uncompromising, high-quality services at a reasonable cost, and customers will follow.

Securance Consulting was launched in 2002 by a former trusted member of a “Big 4” consulting team. The founder felt that his experience at Ernst & Young had provided him with an understanding of the challenges that many different kinds of companies face -- as well as what it would take to master those challenges. Securance set out to deliver outstanding results to each and every client and to ensure that projects were always done right. The mission of Securance was twofold: to convince hundreds of companies about the importance of risk and audit services, and to deliver outstanding services in those areas. Though getting the message out and building an outstanding reputation took persistence, it almost immediately yielded success, as demonstrated by a 20-percent annual growth rate.

To help sustain that growth, in late 2003, Securance Consulting began the process of creating a balanced professional consulting team. Unlike many consulting firms, Securance does not look to hire new college graduates; rather, Securance only hires professionals with a minimum of 10 years’ experience. Generally, that means people with Big 4 experience. Each new hire needs to have special technical strength or leadership skills in order to act as team leader.

From the start, Securance Consulting has worked to provide a presence across all 50 states and has maintained an unwavering commitment to delivering superior results. Securance has never positioned itself as a one-stop shop. Our sweet spot is IT risk and consulting. This focus has impressed client organizations. They know that they can count on Securance to deliver outstanding results without trying to “pad” projects or up-sell them unrelated services. In fact, Securance even offers some services on a fixed-price basis.

Over the past decade, Securance Consulting has built a strong following in the private sector, serving almost 200 organizations as diverse as Lowe’s Home Centers, DelMonte Foods, US Food Service, General Mills, Bob Evans, the power-utility industry and major banks. Between 2009 and 2011, the company also started developing a significant presence in the government sector -- federal, state and municipal -- and continues to grow that part of its practice at double-digit rates.

From its inception, Securance Consulting has been willing to “go the extra mile” to ensure client satisfaction. With that kind of commitment, Securance Consulting clients become true partners. “Our motto is ‘Get it right the first time, every time,’ and that means we want it to be done right, on time and on budget, the first time and every time,” says the founder.
Offeror Qualifications

Securance Consulting has a unique firm structure, which is supported by these points:

Efficiency
One common process and methodology that is consistently applied throughout the firm reflects our philosophy and attitude toward projects: “Get it right the first time...every time.”

Knowledge of the Industry
Our professional consultants are highly competent and continually train to remain current in evolving trends and audit regulatory compliance issues.

Qualifications
Our consultants have a vast array of experience within business, audit services and information technology; they maintain professional certifications. Examples of these certifications are as follows:

- CISA – Certified Information Systems Auditor
- CISSP – Certified Information Systems Security Professional
- CPA – Certified Public Accountant
- GIAC – Global Information Assurance Certification(s)
- CBAP – Certified Business Continuity Professional
- MCSE – Microsoft Certified System Engineer
- SANS – Hacker Techniques, Exploits and Incident Handling

Expertise
We are frequently asked to speak as subject matter experts at select industry conferences and meetings.

Quality Control
Our approach is continuous, with a strong focus on co-development, risk insight, measurement and client satisfaction. Each project performed by Securance is reviewed by an executive independent of the engagement to ensure that all quality and regulatory standards are met. In addition, all preliminary findings will be presented to ISBE’s Management prior to issuance to obtain evaluation and approval.

Client Base
Private and Public Sector Organizations.

Summary of Professional Services
- Compliance (SOX, PCI, GLBA, HIPAA, etc.)
- Governance | Risk | Compliance
- Internal Audit Outsourcing | Co-Sourcing
- Audits and IT Risk Assessments
- IT Security Assessments
- Business Process Review | Redesign
- Vulnerability Assessments and Penetration Testing

Areas of Expertise
- IT Risk Management in the Following Areas:
  - Network Security (LAN, WAN, Wireless)
  - Operating System Security
  - Database Security
  - IT Process Improvement Analysis
  - IT Policy | Procedure Development
  - Disaster Recovery Planning
Offeror Qualifications

Firm Experience and Qualifications
Organizations that have trusted Securence Consulting to perform similar professional services include:
- Teachers’ Retirement System of the State of Illinois
- Frederick County, MD | Frederick Community College
- Louisville – Jefferson County Metro Government
- Houston Community College
- University of Kentucky
- Ohio Public Employees’ Retirement System

Due to confidentiality agreements with our clients, we are not permitted to provide more detailed information about our clients’ operating environments. However, we guarantee that, as evidenced by our client list, Securence is experienced with networks of your size and complexity.

Securence Added Value
- Most comprehensive risk database.
- We review our client’s security posture and provide suggestions about areas that may be improved.
- As a professional services firm, our advanced knowledge of emerging audit guidance and technologies enables us to know about an industry’s risk before our clients…and we are able to freely share this information.

Just a Few of...“The Securence Differences”
- No junior staff. All of our staff have at least 10 years of experience.
- Our Executive Team will have hands-on involvement with every project…not just project management.
- We guarantee 100-percent consistency in executive management and strive for 100-percent consistency in our practice.
- We are not driven by budget requirements….If there is extra work to do, we will do it and will not add billings to the project.
- We are truly our client’s partner. We assist our clients even when we are not under contract.
- Our fee structure is ultra-competitive.
- We focus on financial, operational and technology risk and compliance like no other firm.
Staff Qualifications

Paul Ashe
CPA, CISA, CISSP (pending)
Engagement Manager

Chris Bunn
CISA
Sr. IT Audit Consultant

Chris Cook
CISA, CISSP
Sr. IT Audit & Security Consultant

James McDonald
CISSP, SSCP, CISA
Sr. IT Audit & Security Consultant
Staff Qualifications

Proposed Project Team

Securance Consulting only hires experienced IT audit IT security professionals. We take great care in matching our consultants to each and every engagement so that our customers receive the best possible service while meeting their compliance and management objectives. Each member of every team has 14-plus years' experience, not merely in the services outlined in the Project Scope on pages 7 - 9, but, rather, in performing diverse assessments for public sector leaders.

The team will consist of a combination of personnel with technical and business credentials including CISA, CISSP, MCP, CPA, CEH, CFE, CIA, CISM, CITP and more. We understand the difference between “textbook” and real-world practical security and believe that our consultants’ experience will allow us to effectively strike the balance that is crucial to your organization and your IT security goals.

Securance's proposed project team for this engagement is as follows:

**Paul Ashe, President & Engagement Manager:**
CPA, CISA, CISSP (pending)
Paul, Founder and President of Securance Consulting, has provided hands-on project management and served as Engagement Lead on numerous engagements for the past 14 years. A former IT consultant for Ernst & Young, Paul has leveraged his knowledge and experience into an effective, time- and budget-conscious project management style. An experienced IT audit IT security consultant, Paul is proficient in vulnerability assessments and penetration tests of various systems and differing classes of IPs. He is skilled in a wide range of IT security assessments, including server reviews, firewall configuration analyses, VoIP assessments, physical security reviews and more. Please see his complete resume on pages 58 - 59.

**Chris Bunn, Practice Director & Sr. IT Audit Consultant:**
CISA
Practice Director and Senior IT Audit Consultant Chris Bunn is an expert in IT security, risk management and regulatory compliance. With over 30 years of IT experience, Chris has performed audits and risk assessments for clients in virtually every major industry. He has numerous clients in the government sector and has worked with public educational institutions, including the Teachers' Retirement System of the State of Illinois, the University of Florida, the University of Kentucky and Houston Community College. Please see his complete resume on pages 60 - 61.

**Chris Cook, Sr. IT Audit IT Security Consultant:**
CISSP, CISA
Chris is a Senior IT Security Consultant with over 20 years’ experience in the IT field. Chris has performed IT security services for leaders throughout the public sector, including state and municipal government organizations. He has extensive experience with NIST and ISO compliance standards, as well as other compliance frameworks. Please see his complete resume on pages 62-63.
James McDonald, Sr. IT Audit I Security Consultant:
CISSP, CISA
James is a Senior IT Security Consultant with years of experience identifying, analyzing and successfully combatting IT threats to various systems and platforms. James has a number of public-sector clients, including city and county governments and government-operated agencies. Please see his complete resume on pages 64-65.
Executive Profile

Paul Ashe, CPA, CISA, CISSP (pending)
President and Senior IT Audit I Security Consultant

Senior Executive Professional. 14+ years’ diverse IT experience.
Extraordinary cross-functional management background.
Focused on protecting information for major corporations and other organizations requiring high security.

Overview
Paul Ashe, President of Securance Consulting, has a proven track record of success delivering profit-driven technology solutions and minimizing technology-related risk to top organizations. Over the course of his career, he has taken charge of risk management engagements throughout the public and private sectors - and, in so doing, has established Securance as a leader in the IT field. Paul is an expert in:

- Security Operations
- Systems Engineering
- Risk Assessments

Research
- Business Governance
- Security Management

Experience: IT Audit I Security
Paul has been the lead security professional on numerous attack and penetration engagements. He has significant experience breaching MS Windows and UNIX platforms and perimeter security devices and is proficient in the use of over 75 security tools. His functional experience includes:

- Security Infrastructure Management
- Security Auditing
- Business Impact Assessment
- Risk and Threat Analysis
- Vulnerability Assessments
- Penetration Testing
- VPN Solutions
- IDS Deployment
- SLA and Vendor Management

- "Best Practice" Deployment
- Software Functionality Reviews
- Physical Security Management
- Web-Application Testing
- Mobile Device Reviews
- Social Engineering
- Secure Network and DMZ Architecture Development
- Incident Response

Paul has formulated security policies and procedures to address areas that include:

- Incident Management
- Technical Vulnerability Control
- Patch and Vulnerability Management
- Equipment Security

- Roles and Responsibilities
- Data Destruction
- Firewall Security
- Firewall Security
Executive Profile

Experience: Project-Specific
Paul works closely with public sector leaders to help them improve their security postures and to ensure that best practice controls are used to mitigate known security threats. Recent projects include:
- Teachers' Retirement System of the State of Illinois – IT General Controls Review
- Frederick County, MD I Frederick Community College – Application Security Audit
- Louisville – Jefferson County Metro Government – IT Risk Assessment; Application and Database Reviews
- City of Bowling Green, KY – IT Security and General Controls Audit
- City of Milwaukee, WI – IT Risk Assessment; Network Security Assessment
- University of Kentucky – HIPAA Compliance Review and General Controls Assessment
- Houston Community College – IT General Controls Audit
- Colorado Public Employees' Retirement Association – IT Risk Assessment; System Security Audits
- Ohio Public Employees' Retirement Association – IT General Controls Review
- Pinellas County, FL – IT Security Assessment

Technological Skills
- Platforms - MS Windows; UNIX (SCO, HP-UX, Solaris, Linux, AIX); OS/400; RS/600; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions - MS SQL; MySQL; DB2; SAP; Lawson; MYOB; Oracle; PeopleSoft; JDE; Dynamics; and industry-specific solutions.
- Security Tools - Commercially available and Open-Source tools.

Education, Training and Certifications
- Certified Public Accountant (Florida)
- Certified Information Systems Auditor
- Certified Information Systems Security Professional (Pending)
- SANS Firewall, Perimeter Protection and Security Training
- Bachelor of Science - Accounting and Management Information Systems (Dual Degree)
- Master of Science - Accounting Information Systems
Staff Profile

Chris Bunn, CISA
Practice Director and Sr. IT Audit Consultant

Practice Director and Senior IT Audit Consultant.
30 + years’ experience in IT security, IT risk management and regulatory compliance.

Overview
Chris Bunn, Practice Director at Securance Consulting, is a Senior Management Professional and Certified Information Systems Auditor with over 30 years’ experience in the IT field. He has delivered successful, efficient IT solutions to clients in a broad range of industries, including government and public education, and is a proven expert in IT security, IT risk management and regulatory compliance.

Experience: IT Auditing and Risk Management
Experis Finance – Risk Advisory Services Senior Consultant
• Responsible for the execution of Sarbanes-Oxley (SOX 404) compliance audits for clients in the banking, manufacturing, healthcare and energy industries.
• Completed ISO 27002 compliance, VMware security, Six Sigma and HIPAA compliance audits for a leader in the healthcare industry.
• Performed General Computing Control Audits (GC²R) utilizing COSO and CoBIT audit frameworks.
• Performed segregation of duties reviews, ITIL Service Management (ITSM) V3 evaluations, architecture reviews, business intelligence, IT governance and other information system audits.

University of Florida – IT Audit Manager
• Planned, supervised, and conducted audits of PeopleSoft 8 ERP and Data Warehouse and reporting systems residing on Unix AIX platform; financial systems; operations; advisory services; and other projects.
• Supervised and performed audits of computer systems residing on a variety of hardware platforms and with differing compliance requirements.
• Implemented audit programs across the University’s computer systems.

BDO Seidman LLP – IT Audit Manager
• Responsible for SAP BI and GRC advisory services for mySAP ERP with NetWeaver, Oracle’s PeopleSoft enterprise applications, and other SOA ERP systems. Responsible for business development and project management in technology risk and security, business process improvement, business intelligence and advanced analytics, SOX 404 and JSOX compliance, FISMA compliance, IFRS transition and IT compliance, service organization (SAS70 Type II) and internal audit service lines.
Staff Profile

Experience: Project-Specific
Together with Engagement Manager Paul Ashe, Chris helps top organizations identify, analyze and, ultimately, remediate technology-related risks. His recent projects include:
- Teachers' Retirement System of the State of Illinois – IT General Controls Review
- Houston Community College – IT Audit
- Ohio Public Employees' Retirement System – IT General Controls Review
- Pinellas County – IT Security Assessment
- Kissimmee Utility Authority – IT Risk Assessment
- University of Kentucky – HIPAA Compliance Review and General Controls Assessment

Technical Skills
- Platforms - MS Windows; UNIX; OS/400; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions – MS SQL; Oracle, DB2; MySQL; SAP; Oracle; PeopleSoft; Lawson; JDE; Dynamics; and industry-specific.
- Security Tools - Commercially available and Open-Source tools.

Education, Training and Certifications
- Certified Information Systems Auditor
- Master of Science - Management Information Systems
- Bachelor of Science - Computer Science for Business
Staff Profile

Chris Cook, CISSP, CISA
Sr. IT Audit I Security Consultant

Senior IT Audit I Security Consultant. 20 + years' diverse IT experience.
Significant expertise with NIST, ISO and other regulatory compliance frameworks.

Overview
Senior IT Consultant Chris Cook brings extensive experience in IT security, risk analysis and regulatory compliance to this project team. Before joining Securance seven years ago, he worked at the NASA AMES Research Center, at BlueCross BlueShield as a Project Manager and at IBM as a Managing Consultant. He is an expert in:

- Security Evaluations
- Risk Assessments
- Vulnerability Assessments
- Penetration Tests
- UNIX I Linux and Windows Server Reviews

Experience: IT Audit I Security
NASA Ames Research Center
- Prepared certification and accreditation packages according to NIST guidelines. Packages included risk assessments, security plans and contingency plans.

BlueCross BlueShield of Kansas City – Project Manager, CoBIT Controls Assessment
- Developed project to assess CoBIT controls for Model Audit Rule (MAR) compliance.
- Assessed corporate policy infrastructure.

IBM – Managing Consultant, Security and Privacy Practices
- Conducted security evaluations according to ISO and NIST standards.
- Performed application vulnerability assessments using WebInspect software.
- Reviewed internal clients' practices for compliance; recommended appropriate solutions.

Experience: Project-Specific
Chris works closely with our Engagement Manager, Paul Ashe, to help clients in every industry, including government, improve their security postures and to ensure that best practice controls are used to mitigate known security threats. Recent projects include:

- Kissimmee Utility Authority - IT Risk Assessment
- City of Grants Pass, OR - Network Security Assessment
- City of Richmond, VA - Network Security Assessment
- City of Tacoma, WA (Tacoma Water) - Cyber Security Assessment
- Maryland National Capital Park and Planning Commission - Vulnerability Assessments
- Orange County Sanitation District - Security Assessment
Staff Profile

Technological Skills
- Platforms - MS Windows; UNIX (SCO, HP-UX, Solaris, Linux, AIX); OS/400; RS/600; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions - MS SQL; MySQL; DB2; SAP; Lawson; MYOB; Oracle; PeopleSoft; JDE; Dynamics; and industry-specific solutions.
- Security Tools - Commercially available and Open-Source tools.

Education, Training and Certifications
- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- SOA Fundamentals and Security
- SANS Track 4 - Hacker Techniques, Exploits and Incident Handling
- SANS Track 6 - Securing UNIX/Linux
- SANS Track 12 - SANS Security Leadership Essential
- SANS Securing Solaris Using the Center for Internet Security Benchmarks
- SANS Track 7 Auditing Networks, Perimeters and Systems
- Department of Energy Cyber Security Training & Basic Security Survey
- Network Associates Sniffer University
- Bachelor of Science – History
Staff Profile

James McDonald, CISSP, CISA
Sr. IT Audit I Security Consultant

Senior IT Audit I Security Consultant. 15 years’ experience analyzing and combatting IT-related threats. Significant expertise in all facets of IT security, risk analysis and systems administration.

Overview
Over the course of his career, Senior IT Consultant James McDonald has attained proficiency in IT assessments ranging from vulnerability assessments and penetration tests to compliance testing and policy I procedure reviews. He has been with Securance since 2010.

Experience: IT Audit I Security
James boasts expertise in all areas of IT security and in auditing, regulatory compliance and business continuity planning. His strengths include:
- Security Auditing
- IT Risk Analysis
- Vulnerability Assessments
- Penetration Tests
- Web-Application Testing
- Server Reviews
- Internet Security Assessments
- Application Security Assessments
- IT Policies I Procedures
- Incident Response, Disaster Recovery and Business Continuity Planning
- Sarbanes-Oxley (SOX) Compliance

Experience: Project-Specific
Securance Consulting - Senior IT Consultant
- Works closely with Engagement Manager Paul Ashe to identify, analyze and remediate IT risks.
- Recent clients include Louisville-Jefferson County Metro Government (vulnerability assessment and penetration test), Liberty Savings Bank (IT security assessment) and Performance Software (IT security and consulting services).

APPTIS, Inc. - Information Assurance Engineer, MacDill Air Force Base, Tampa, FL
- Analyzed threats based on information in open-source and intelligence reports. Deployed effective countermeasures against threats; created threat advisories.
- Analyzed network and system changes I reconfigurations with regards to IT security.
- Established security regulations and directives.

Kforce, Inc. - Security Analyst III
- Responsible for systems security, vulnerability and risk assessment, disaster recovery and business continuity planning, and Sarbanes-Oxley (SOX) 404 internal controls.
- Designed effective SOX controls. Worked closely with business units and internal I external auditors to improve relevant business processes and controls. Conducted quarterly access control audits.
- Conducted quarterly security configuration audits (automated and manual testing) in a mixed HP-Unix 11i, Redhat Linux and Windows environment.
- Developed, tested and improved security and incident response policies and procedures.
Staff Profile

Experience: Project-Specific (continued)

Kobie Marketing - Cross-Platform Security Administrator
- Responsible for all aspects of IT security in a mixed Redhat Linux, HP-Unix and Windows environment, including network security, system and application hardening, intrusion detection and prevention systems, firewall configurations, patch management procedures, security awareness training and IT policies and procedures.
- Performed regular risk analyses and security assessments.
- Developed, tested and improved security policies and procedures, incident response protocols and disaster recovery and business continuity plans.

Technological Skills
- Platforms - MS Windows; UNIX (SCO, HP-UX, Solaris, Linux, AIX); OS/400; RS/600; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions - MS SQL; MySQL; DB2; SAP; Lawson; MYOB; Oracle; PeopleSoft; JDE; Dynamics; and industry-specific solutions.
- Security Tools - Commercially available and Open-Source tools.

Education, Training and Certifications
- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- Systems Security Certified Practitioner
- GIAC Certified Incident Handler
- Bachelor of Science - Management Information Systems
- Associate of Arts
Laguna Blanca.
The Next Step

What the ISBE Should Expect

Securance provides the best fit to the ISBE for this assignment for the following reasons:

Qualifications – the team we proposed includes senior leadership from the firm. Our team leaders and staff are Certified IT Security Professionals with intimate knowledge of the technologies in your environment.

IT Security Expertise – as a firm of Senior IT Security Consultants, we intimately understand information technology and internal controls. Our methodology is designed around global best practices. We are experts already...

Sustained Improved Controls – only the Securance approach includes a sustainable improved internal controls environment solution. Our team will identify and share with the ISBE processes and improvements to current processes that will help improve the organization's internal controls on an ongoing basis.

Experience – key members of our team of consultants are former “Big 4” IT security consultants. In addition, our team has real-world experience that enables us to differentiate between “textbook” controls and real-world practical controls. Your reports will not contain recommendations that cannot be implemented in your environment.

High Quality Deliverable – our Management Report is tailored to the various audiences that will receive it. The report contains an easy-read Executive Summary with no technical jargon. Yet, it also contains sufficient detail that your team of system administrators and engineers can implement our proven recommendations.

True Partnership – we are long-term partners with staying power. We will not simply leave when the assignment is over. We will be there to support the remediation and ensure the implementation of our recommendations is successful. When needed, we will roll up our sleeves and participate in the implementation. The ISBE will become a client of Securance for life...this means you can contact us for support or technical advice, free of charge, even when not under contract. That is the Securance definition of a partner!

It is easy to see why Securance should be the firm of choice!
The Next Step

Assumptions We Have Made:

- Securance Consultants will have full access to all client participants and personnel, as required through the duration of the engagement.
- The ISBE's personnel will provide Securance Consultants with all information requested to complete this engagement in a timely manner.
- The ISBE's Project Coordinator will hold meetings with the Securance Engagement Manager, as necessary, to assess the project's progress.
- ISBE Management will be responsible for all remediation of identified vulnerabilities and risks.

Logistic Requirements:

- Securance Consultants will need adequate workspace and Internet connections while on site to access email and other firm resources.
- Securance Consultants will need access to a dedicated phone extension and printing capabilities.

What's Next for the ISBE?

- Engage Securance Consulting today!
- Conduct a planning session.
- We’ll hit the ground running, with interviews scheduled in advance of our site visit and pre-defined client assistance requirements. We’ll adjust our schedules to ensure minimal disruption to your staff.
- Fast return on investment as you realize the benefits of engaging Securance Consulting.
SAMPLE STATUS REPORT

Client Name
<<Project Name>> Status Report

Project Detail

Project Manager
Reporting Week
Overall Project Status

Project Status Key: Green—On Target, Yellow—At Risk, Red—Project will not finish on-time

<table>
<thead>
<tr>
<th>Activity for this Reporting Period</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Planned Activities for Next Reporting Period</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Engagement Manager</td>
</tr>
<tr>
<td>Sr. Consultant</td>
</tr>
<tr>
<td>Sr. Consultant</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project Issues and/or Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue #</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Request</td>
</tr>
<tr>
<td>----------------</td>
</tr>
</tbody>
</table>
### Project Milestones

<table>
<thead>
<tr>
<th>Status</th>
<th>Milestone</th>
<th>Target Date</th>
<th>Revised Date</th>
<th>Actual Date</th>
<th>Reason Not Met*</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Key Meetings This Week

<table>
<thead>
<tr>
<th>Meeting Date &amp; Time</th>
<th>Purpose</th>
<th>Attendees</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>