HACC, CENTRAL PENNSYLVANIA’S COMMUNITY COLLEGE
REQUEST FOR PROPOSAL
#09-10
BUSINESS RISK ASSESSMENT / INTERNAL AUDIT SERVICES
ADDENDUM #1
ANSWERS TO QUESTIONS
SEPTEMBER 11, 2008

Question 1: I am requesting some clarifications in the scope of work regarding RFP 09-10 Business Risk Assessment / Internal Audit Services. Are you looking for IT auditing and assessment services or is this financial auditing and assessment services? If this RFP is for IT work, can you please be more specific as to work you are looking to have completed, such as penetration testing, vulnerability assessment, etc. If you have a more specific scope of work, that would be greatly appreciated.

Answer 1: This RFP is for financial assessment and internal auditing services.

Question 2: Have you conducted prior risk assessments?
If so, will the results be provided to the service provider?

Answer 2: This is the first formal assessment process.

Question 3: Do you have expectation on what level of personnel (management) that you expect to be interviewed in the risk assessment process?
I.e. Executives and Board of Trustees only
I.e. Executives, Board of Trustees, Management and the HACC Foundation

Answer 3: Final findings and recommendations will be presented to The Finance Committee of the Board of Trustees. We do anticipate a broader interview process in the risk assessment.

Question 4: Is the HACC foundation considered part of the risk assessment and potential audit area[s]?

Answer 4: Yes

Question 5: Are your policies and procedures developed for all processes and current throughout HACC?

Answer 5: With SAS 104-111 guidelines, this past year we have made a concerted effort to have desktop manuals and standard operating procedure documents updated. At this time these documents are current for all of the Finance areas (Accounting, AP, Budget, Student Accounts).

Question 6: Has HACC ever had an Internal Audit Department?

Answer 6: No

Question 7: Does the Board of Trustees/Management have any internal audits broken out by financial, operational, compliance and IT?
Answer 7: No

Question 8: Are there any major upgrades to Banner planned?

Answer 8: We are planning to upgrade from version 7 to version 8 in the fourth quarter of 2009. We are also planning on implementing SunGardHE’s Luminis integrated portal solution in 2009.

Question 9: Does the University conduct an internal / external vulnerability assessment at least annually and does it have any of the following as part of the infrastructure: DMZ and IDS (host and / or network based)?

Answer 9: In conjunction with PCI compliance, the College is expecting to undergo external vulnerability assessments quarterly. We do not currently utilize a DMZ or IDS, but will likely be implementing some version of both in conjunction with becoming PCI compliant.

Question 10: Is the IT environment more focused on preventive or detective controls?

Answer 10: The ITS Department does utilize a preventive focus wherever possible, such as a security policy of least-privilege and restricting external access to our internal network only as needed. We do use some detective controls when investigating variances to typical usage of resources or when contacted by other departments regarding personnel issues.

Question 11: Are there any significant IT functions that are outsourced to a third party? If so, which functions and how does management get comfortable on the controls at these environments?

Answer 11: No, all significant IT functions are managed in house.

Question 12: Is there a requirement to be Payment Card Industry Data Security Standards (PCI / DSS) compliant? If so, what level merchant are you considered by your merchant bank?

Answer 12: Yes, there is a requirement for PCI compliance. We are considered a Tier 3 merchant.

Question 13: Has the University experienced any significant security breaches / attacks within the past year? If so, have these incidents been reported to senior management and / or the board?

Answer 13: No

Question 14: Has a Risk Assessment ever been completed for HACC? If so, will the chosen firm be able to use the existing Assessment as a starting point?

Answer 14: No

Question 15: Has an Internal Audit ever been completed for HACC?

Answer 15: No
**Question 16:** On Page 17 of the RFP, under Reference and Other, there is a signature block. Could you please clarify the purpose of this signature block, for example would you like this signature block completed by us at the end of the proposal or would you like each reference to complete the signature block?

**Answer 16:** This should be signed by an authorized representative of your firm to confirm to the accuracy of the answers provided in this section.

**Question 17:** How many firms have received notice of the RFP?

**Answer 17:** HACC notified 28 firms of the Request for Proposal.

**Question 18:** Who is your external auditor?

**Answer 18:** Smith Elliott Kerns and Company, LLC (SEK & Co), Chambersburg, PA

**Question 19:** Do you currently have an internal audit function?

**Answer 19:** No

**Question 20:** Has a risk assessment been performed previously?

**Answer 20:** No

**Question 21:** Can you clarify the statement in Section X, IV, b, 5 to describe "Provide emergency fraud audits"? This would be our ability to provide fraud investigations?

**Answer 21:** Yes

**Question 22:** Can you clarify your intended definition of business risk? Is it primarily financial risk, or is the scope to be enterprise risks, such as operational, fraud, strategic and compliance?

**Answer 22:** Primarily financial risk. A part of this financial risk assessment should entail some elements of these other enterprise risks.

**Question 23:** Our firm has extensive experience in risk assessments and internal audit services, however we have limited experience in the field of higher education. Will this fact exclude us from consideration and if not, how significantly will it impact your consideration of our proposal?

**Answer 23:** Your firm would not be excluded. While higher education / non-profit experience is preferred, it is a sub-factor of overall experience when reviewing proposals.

**Question 24:** How do you plan to handle changes in scope for the internal audit plan that might result from the actual completion of the risk assessment?

**Answer 24:** We understand you cannot know the specific audits required until the assessment is completed and we have our prioritized list of risks. For budgeting purposes we anticipate setting an annual budget for internal auditing services, with an annual internal audit plan developed based on the College’s priorities.

**Question 25:** Will there be any limitations to the scope of the business risk assessment?
Answer 25: See # 22

**Question 26:** Do you have an Organization Chart and Strategic Plan that you can share?

**Answer 26:** Both our Organization Charts and Strategic Plan are under review and not currently available. Our last strategic plan can be seen at our website hacc.edu under About Us / Administration / Strategic Plan.

**Question 27:** Has funding been allocated to the project for the current fiscal year?

**Answer 27:** Yes

**Question 28:** Of the key vendor differentiators identified in the RFP (Firm Profile, Staff and Experience, Scope and Approach, References and Cost) what would be considered the important factors to the College’s selection process?

**Answer 28:** All except cost which is secondary.

**Question 29:** Which “business office” functions (accounting & finance, student billing, payroll processing, etc) are performed independently at each of the five locations identified (Gettysburg, Harrisburg, Lancaster, Lebanon and York) and which functions, are performed at a central location?

**Answer 29:** All of the functions mentioned are centralized on the Harrisburg Campus. Of course, there are certain functions in each that are decentralized as with the approval of time sheets and invoices, cashiering, etc.

**Question 30:** Do any locations house an academic specialty not found at the other locations (school of business, school of fine arts, etc.)?

**Answer 30:** Most programs are offered at each campus to some extent. Students in certain programs at a smaller campus may need to attend classes at a different campus to complete that program.

**Question 31:** Does the College outsource any of its auxiliary service functions, such as the campus bookstore or foodservices?

**Answer 31:** We run our bookstores, conference center and museum store. Our food service operation (except in the conference center) is outsourced.

**Question 32:** Does the College manage its endowment or is the endowment managed by an external party?

**Answer 32:** External parties

**Question 33:** What is the name of the CPA firm that currently performs the College’s independent audit?

**Answer 33:** Elliott Kerns and Company (SEK), Chambersburg PA
Question 34: Is the College’s external auditor planning to place any level of reliance on the work performed with regards to the risk assessment or internal audit projects?

Answer 34: The firm has done its own risk assessment for their auditing purposes. There has been no discussion of this assessment or its results being a factor in their audit plan.

Question 35: Has the College received a SAS 112 letter (communication on internal controls) from its external auditor? If so, did the letter call out any significant deficiencies or material weaknesses in internal controls?

Answer 35: There was no specific SAS 112 letter.

Question 36: Has the College received a management letter from its external auditor? If so, were any specific points regarding internal controls, risk or internal audit included?

Answer 36: Our Board of Trustees receives a management letter annually.

Question 37: In general, does the College believe it has any significant deficiencies or material weaknesses in internal controls? If so, please describe.

Answer 37: We are unaware of any, but want to be proactive in complying with certain SOX recommendations for Higher Ed.

Question 38: Has the college ever performed a risk assessment? If so, what was the focus (financial, business, operations, etc.)? What were the results? Were any specific processes called out as high risk?

Answer 38: No

Question 39: Has the College identified any significant risks to the organization? If so, please describe.

Answer 39: No

Question 40: What is the desired focus of the current risk assessment (financial, business, operations, etc.)?

Answer 40: Primarily financial risk. A part of this financial risk assessment should entail some elements of these other enterprise risks.

Question 41: Has the College identified the key processes to be included as a part of the risk assessment, based upon the desired focus? If so, please describe the key processes identified.

Answer 41: No

Question 42: Is there a specific time line for completion of the risk assessment desired by the college?

Answer 42: We would hope to have it completed this FY if possible, but have no set timeline.
Question 43: In the College’s opinion, would the scope of the risk assessment encompass all locations?

Answer 43: Yes

Question 44: Please describe the College’s and expectations surrounding an outsourced internal audit function.

Answer 44: We anticipate a priority driven annual internal audit plan with results and recommendations presented to the Finance Committee of the Board.

Question 45: Has the College considered a potential scope for its outsourced internal audit projects (i.e. financial, business, operational, etc.)? If so, please describe the desired scope.

Answer 45: No

Question 46: Are there currently any important internal audit projects being considered by the College?

Answer 46: No

Question 47: Is there a specific time line for completion of potential internal audit projects desired by the college?

Answer 47: Not at this time.

Question 48: What are the main business applications used by the College?

Answer 48: SunGard HE's Banner suite of higher ed applications, Novell NetWare and GroupWise, and Blackboard Campus Edition.

Question 49: Has the College ever conducted an IT risk assessment in the past? If so, when was it conducted and what were the major findings?

Answer 49: No

Question 50: Does the College follow an IT governance methodology?

Answer 50: Not applicable

Question 51: Does the College utilize a framework of control objectives for IT general computer controls? If so, which framework?

Answer 51: Not applicable

Question 52: Does the College outsource any component of its IT function to a service provider?

Answer 52: No

Question 53: Describe the College’s network topology.
Answer 53: The college is setup using a Ethernet topology in a star configuration. All of our buildings and regional campuses are connected to our main data center. The college is actively engaged in increasing the minimum speed to all regional locations to 100 megabit Ethernet.

Question 54: How many servers does the College maintain?

Answer 54: The college maintains and operates between 100 to 150 servers.

Question 55: What server operating systems are used by the College?