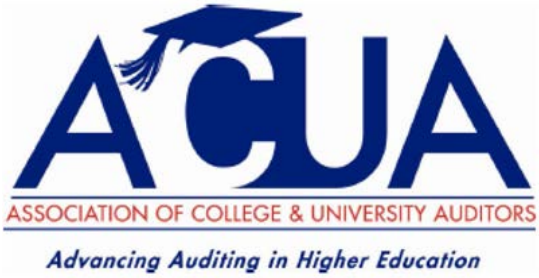



AUGUST 2017

# CONDUCTING AN INTERNAL AUDIT RISK ASSESSMENT USING AN AUDIT UNIVERSE AND RISK FACTOR SCORING APPROACH

## A PRACTICAL GUIDE FOR INTERNAL AUDIT DEPARTMENTS OF HIGHER EDUCATION INSTITUTIONS

David Mosca - Director of Internal Audit, University System of Maryland
Courtney Ruckert - Audit Manager, Emory University
Chris Garrity - Director of Internal Audit, Saint Joseph's University
Donald A. Temple - Audit Manager, State University of New York System Administration
Al Smith - Vice President, University Registrar, (Formerly Vice President of Internal Audit), Strayer University

# Table of Contents

# INTRODUCTION

Why perform a risk assessment as a basis for putting together internal audit's plan of engagements or activity? **For most internal audit leaders, the risk assessment has been, at the very least, a best practice or a prescribed professional standard. However, the most compelling reason to conduct these risk assessments is that it will help the internal audit executive be more effective at his/her job**. The primary benefit of conducting the risk assessment is to increase the likelihood the internal audit function will perform a higher percentage of impactful audit engagements. The secondary benefit is that the process will help build relationships with management.

Regardless of the size and/or complexities of our organizations, the basic framework for internal audit performing risk assessments has been relatively static over the years. That being:

Step 1 – Identify the audit universe;

Step 2 – Ranking or scoring the audit universe based on various risk factors; and

Step 3 – Choosing which audit areas to include in the audit plan.

While this seems like a straightforward process, guidance from our professional standards on how to carry out these steps is sparse to say the least. This lack of precise guidance has left internal audit leaders with some frustration as to how best to conduct worthy risk assessments. With this in mind, the primary objective of this white paper is to:

**Provide useful guidelines, resource information, and leading practices that can be used by all internal audit leaders in higher education by optimizing their risk assessments for their own organizations.**

# GETTING STARTED

The risk assessment takes subjective, professional perspectives and puts them through an objective framework that is organized in a way that will help you determine where to best allocate your resources.

It must be understood that there is no universal step-by-step methodology to follow when conducting the risk assessment. Audit leaders must decide on a methodology that best fits their organization and their own professional judgment and values. This paper will provide different pieces of the methodology that chief auditors can choose from in developing their own process. We will also put these methodologies into some context, which is based upon practices our ACUA leadership members currently utilize. Our tables are based on a 2016 survey of more than 100 ACUA leaders across the nation. Approximately 70% of these participants are from audit shops of four (4) auditors or less.

| **What size is your internal audit department?** | | |
|---|---|---|
| **Answer Options** | **Response Percentage** | **Response Count** |
| Small (1 – 4 Auditors) | 65.8% | 73 |
| Medium (5 – 15 Auditors) | 27.0% | 30 |
| Large (>15 Auditors) | 7.2% | 8 |
| | *answered question* | **111** |
| | *skipped question* | **1** |

If you have not conducted a risk assessment for your organization, we urge you to overcome any roadblocks and not miss out on any opportunities that may be realized from the activity. Understand that the first assessment is often the most challenging and that the more risk assessments you perform, the better you will become. One must also accept the fact the process is not perfect, but you will achieve benefits.

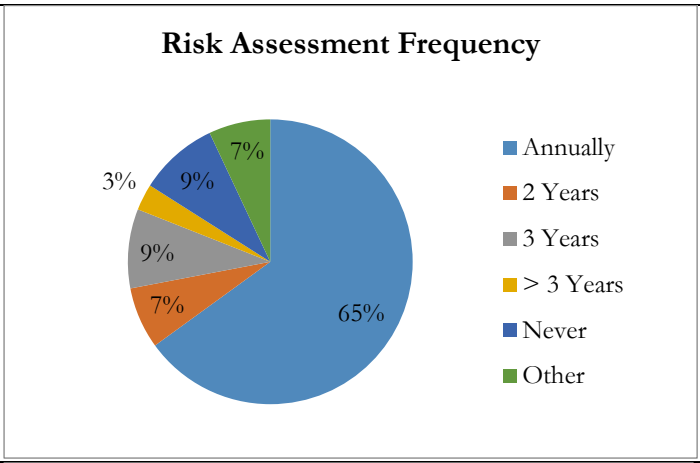
# SOME QUESTIONS TO CONSIDER

*Frequency*

**How frequently should you complete the risk assessment?**

Most Professional Standards recommend or require that a risk assessment be completed annually,

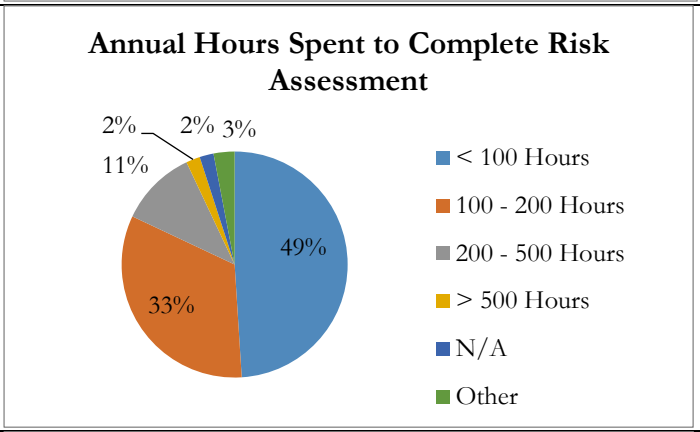
ACUA Constituents: Majority indicated completed annually.




*Effort*

**How many hours should you devote toward completing the risk assessment?**

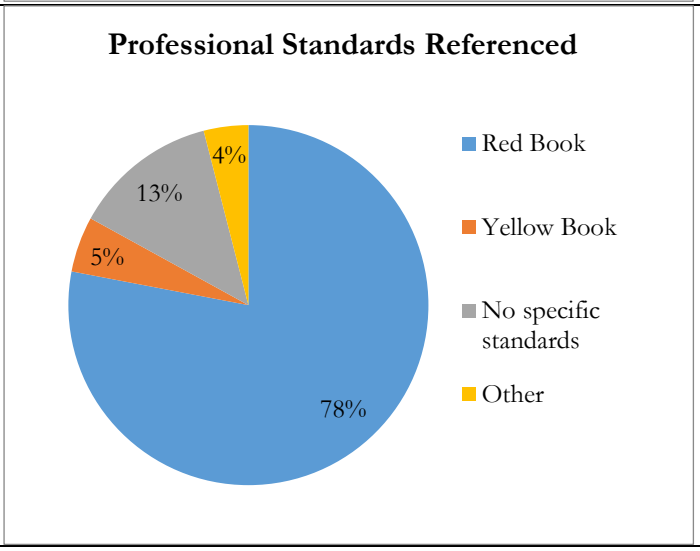
ACUA Constituents: Majority indicated annual hours were less than 100.




*Professional Standards*

**Does your organization follow specific professional standards?**

ACUA Constituents: Majority indicated the Red Book, published by the Institute of Internal Auditors (IIA) as the professional standards most commonly referenced.



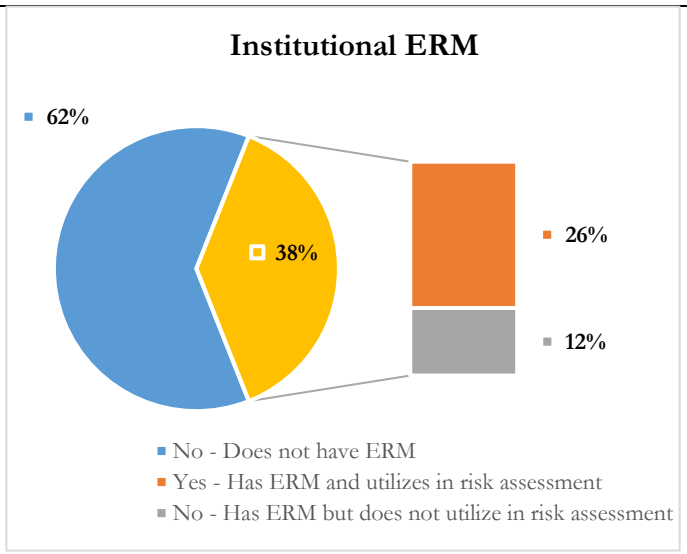
*Enterprise Risk Management (ERM)*

**Does your institution/organization have an ERM program?**

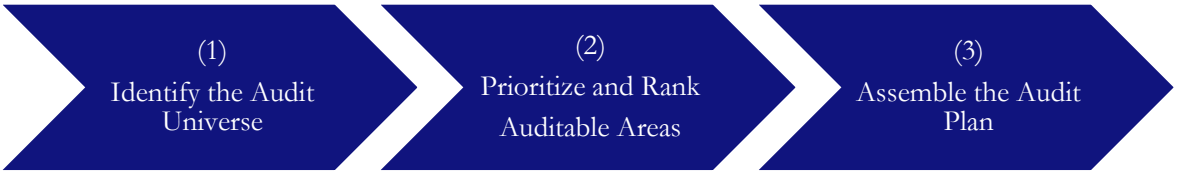
Yes – 38%
No – 62%

**If yes, do you utilize the ERM program in your risk assessment?**

Yes – 26%
No – 12%




# CREATING A RISK ASSESSMENT FRAMEWORK



## STEP 1: IDENTIFYING THE AUDIT UNIVERSE


The audit executive must decide which method work best for their organization.

Developing the audit universe requires each organization to develop and maintain a list or register of auditable entities that can be utilized and updated from year to year.

An excellent resource that identifies scores of audit areas is ACUA's Risk Dictionary available on ACUA's website. Also in Appendix A, is a register of auditable areas in higher education.

## STEP 2: PRIORITIZING AND RANKING THE AUDITABLE AREAS

Once you have your risk universe documented, you may begin the second step of the risk assessment process, which is ranking and scoring the auditable entities based upon various risk factors.

It should not be expected that each and every entity in the audit universe be scored. Rather the audit executive may judgmentally rank the top risk areas that will ultimately be scored. There is no one magic number. In our survey, we asked the ACUA collective how many risk areas were scored when completing their risk assessments. The results are below.

| How many risk areas do you score/rank in your risk assessment (risk areas = auditable entities/units/etc.)? | | |
|---|---|---|
| **Answer Options** | **Response Percentage** | **Response Count** |
| 0 – 20 | 16.2% | 18 |
| 20 – 30 | 9.9% | 11 |
| 30 – 50 | 19.8% | 22 |
| More than 50 | 47.7% | 53 |
| N/A | 6.3% | 7 |
| | *answered question* | **111** |
| | *skipped question* | **1** |

Depending on your organization, you may set up different audit categories that can be scored separately. For example, system audit functions may score each university separately, and those organizations with hospitals may score the hospital risk areas separately from a university. So you too might score separate audit disciplines such as IT/IS security, fraud risk, financial risk or construction risks. Each depends on the audit needs of the organization.

Once the number of auditable entities of higher risk have been identified, we can begin the process of scoring the risks for impact and likelihood. In our survey, we asked the ACUA collective which various risk factors they use and how many risk factors are used in their scoring matrices. The results are below:

| What risk factors do you use when scoring risks? | | |
|---|---|---|
| **Answer Options** | **Response Percentage** | **Response Count** |
| Health and Safety | 38.4% | 43 |
| Financial | 88.4% | 99 |
| Public Image and Reputation | 79.5% | 89 |
| Outside Influences | 30.4% | 34 |
| Strategic Risks | 58.0% | 65 |
| Volume/Size – Number of employees, money, students | 55.4% | 62 |
| Change | 56.3% | 63 |
| Complexity | 58.9% | 66 |
| IT System Risk | 53.6% | 60 |
| ERM Results | 25.0% | 28 |
| Time since last audit | 50.9% | 57 |
| Results of previous audits | 54.5% | 61 |
| N/A | 6.3% | 7 |
| Other (See Appendix E For "Other" List) | 33.9% | 38 |
| | *answered question* | **112** |
| | *skipped question* | **0** |

| How many different risk factors do you utilize when scoring/ranking risks? | | |
|---|---|---|
| **Answer Options** | **Response Percentage** | **Response Count** |
| 3 | 7.2% | 8 |
| 4 | 7.2% | 8 |
| 5 | 22.5% | 25 |
| 6-8 | 24.3% | 27 |
| Over 8 | 26.1% | 29 |
| N/A | 12.6% | 14 |
| | *answered question* | **111** |
| | *skipped question* | **1** |

When scoring the auditable entities, one should keep in mind the likelihood and impact the risk factor may have. Our survey identified the usage of the following rating scales:

| What risk rating scale do you utilize when scoring risks? | | |
|---|---|---|
| **Answer Options** | **Response Percentage** | **Response Count** |
| Low, Medium, High | 54.5% | 60 |
| 1 to 3 | 5.5% | 6 |
| 1 to 5 | 27.3% | 30 |
| 1 to 10 | 2.7% | 3 |
| N/A | 4.5% | 5 |
| Other (please specify) | 5.5% | 6 |
| | *answered question* | **110** |
| | *skipped question* | **2** |

In our Appendix B, we have examples of different scoring matrices, including one for IT/IS Security. As you complete your own score sheet(s), the principle of the assessment is that those areas with the highest scores should be first in line to be audited. However, one should always perform a reasonableness review of the scoring results. Sometimes an area that has a high overall score may not be of the highest risk and vice-versa. One should ask the questions:

1. Do the scores make sense?
2. Do you have policy driven engagements?
3. Do you have management requests?
4. Have areas been recently audited?
5. Is the plan in your comfort zone?
6. Can you compare your plan to peers?

Based on your answers, reevaluate the scoring results and adjust if necessary.

## STEP 3: ASSEMBLING THE AUDIT PLAN

After you have completed the reasonableness review, you can start to finalize the audit plan. This is generally a straightforward process of selecting the highest risk areas and aligning this with your audit resources or staffing. As you do this, it is important to consider the expectations of how much the audit plan is to be completed, and that the plan should be flexible to address emerging risk that may come about during the year. Keep a level of completion in mind when assembling the plan for planning purposes and to set expectations for your stakeholders (Audit Committee or other Direct Report(s)).

While productivity varies some for every audit shop, the Chief Audit Executive (CAE) should understand how much work can be completed by his or her staff in a given year. Similarly, the CAE should have a general idea as to how many hours each audit engagement should take. It is fairly straightforward math at this point. For example, if your staff auditor can produce 1500 audit hours a year, they should be able to complete five 300-hour audit engagements. Consider that you want to complete 85% of your audit plan; you can confidently schedule your top six 300 hour audit engagements or your top eighteen 300 hour audit engagements if you have a staff of three auditors.

Now you can start to populate your audit plan. You can use a spreadsheet of engagements for a multi university system or a list of engagements for a single institution.

As a final note, do not forget to include your follow up audit commitments and the audits that are likely to be in process at the start of your audit calendar when budgeting your available hours.

## GAINING FEEDBACK FROM MANAGEMENT

A cornerstone of the risk assessment process is gaining feedback from management. Two of the most common methods of gaining this feedback are through interviews and surveys. While there is a litany of standard questions available and used when conducting interviews and surveys, there are also hazards of losing credibility if executed poorly. Often we lose sight of what we are trying to achieve. While we would like our audience to see the value in what we do and why we conduct audits, remember it is the audit executive who is looking for information, not the other way around. If we are expecting more from one interview or survey, we are likely to be disappointed.

From this perspective, we are reminded of two anecdotes. The first is a comment made several years ago by a fellow auditor. Wanting to get out of auditing, he landed a job selling medical equipment. In catching up with him years later, he was asked how his job was going. He replied that he had learned that the only people that folks want to see walk through their doors less than auditors are salesmen. The other is that it is important to see things as they are, rather than how they should be. What is to be learned from this? Entering a discussion as both an auditor and a salesman is a daunting task and we should not strive to change people's perspectives to match our own.

Do not fall into the trap of thinking that we can achieve the residual benefits of building long-term relationships of trust and understanding of each other's values in one interview. Look to the long-term strategy of delivering quality audit products and being a person who is consistently trustworthy over time.

So how do we overcome these hurdles, especially if we have little experience? The first step is to understand that we need management's help to complete our risk assessment and they are not necessarily open to being audited or sold on the importance of our value. However, it is often human nature to want to help others. If we begin our discussion by asking the manager for his/her help in this thing we call a risk assessment, you will likely see more positive responses.

We also want to be very up front and transparent in our discussions/surveys. Be clear that this is a process to help us identify areas to audit. If the manager feels betrayed that you are auditing an area that would have been left alone otherwise, you can severely damage the relationship and it may never recover. If during your interview or reviewing survey results, you see an area that might cross the "betrayal" line, seek more input from that manager. Get their thoughts and hopefully their buy in that a particular area, which surfaced in the interview/survey, would benefit from an audit. If the manager is voicing his/her concerns about this area being audited, it is time for the audit executive to look at their own values as to whether to conduct an audit or not. You may be operating in an important area this year, but will be missing out on several important areas in the years to come. No small dilemma. To help guide you through such a dilemma, fall back on your values. Is personal safety or other personal harm at risk, is your organizations reputation at risk, is there a high risk for fraud, etc.? Putting these in perspective will help you with your final decision. If you decide to conduct the audit in this area, be up front with the manager. Let him/her know the position you are in and most will understand and appreciate your being forthright.

Conduct interviews in a way that fits your own personal and professional style. Some of us have the gift of gab, some of us have the gift of listening and some of us have the gift of eloquence. Whether you conduct your interview with a list of questions or in a freeform discussion, it is important to be yourself and you will be successful.

The auditor must also understand that many employees, including high-level managers, may not understand what controls are, what risk is, what a risk assessment is, etc., and may need these explained and defined upfront. In bridging this potential gap, ask the age-old questions such as "what keeps you up at night," "what worries you the most," and "what do you think could be newsworthy?"

Be thoughtful with your surveys. A poorly designed survey will often result in poor responses and loss of credibility if the respondent becomes frustrated with the questions. Some dos and don'ts:

- Make the survey easy to complete;
- The survey should not take more than 10 to 15 minutes to complete;
- Understand yourself and what information you are trying to get from the survey and ask questions accordingly;
- Do not ask questions that require the individual to perform research or put together a report;
- Do not ask for information that you do not need. If you want information like budget reports, organizational structure, or the like, ask for this information outside of a survey; and
- Do not just read the survey before sending it out, but take the survey yourself. If you get frustrated answering the questions, there is a high likelihood your audience will get frustrated as well.

(See Appendix C – Examples of Survey Questions)

## INCORPORATING ERM INTO THE RISK ASSESSMENT PROCESS

The primary benefit of incorporating your organization's ERM program into Internal Audit's risk assessment is that it provides a source for identifying auditable entities into the risk universe. It can also serve as a valuable indicator of various hot spots, which may not be readily identified through other risk assessment methods.

Depending on the level of detail of your organization's ERM framework, the volume of ERM risks can be significant. While management may have narrowed the lists of risks into a "top X list," it is up to the Chief Audit Executive to use his/her professional judgement to identify those high-risk areas in ERM's risk inventory to include with internal audit's rating/scoring process.

Incorporating your institution's ERM into your overall risk assessment includes the following three components:

### 1. Understanding your institution's ERM process and methodology

The ERM process provides a window into management's perception of current and emerging risks within their area or domain. Management's risk selection methodology is therefore important to understand as it provides perspective into their justification and rationale in selecting the stakeholders, identifying the risks, ranking the risks, and developing the risk remediation plans. Furthermore, it is a valuable indicator of various hot spots, which may not be disclosed through other risk assessment methods such as leadership interviews, risk assessment surveys, etc. This holistic understanding will support your overall evaluation and prioritization of the ERM risks.

Of course, there can be limitations to the ERM process, which are important to consider, especially since you may be leveraging the top ERM risks to develop your audit plan. Examples of such limitations to the ERM process are as follows:

a. Limitations on recognizing new/emerging risks from year-to-year;
b. Risk rankings may be inherently subjective; and
c. Risk remediation plans may not be in place and/or may not be adequately functioning.

Once you have an understanding of the ERM process including its inherent limitations, next evaluate the list of ERM risks (i.e., ERM risk inventory) for potential inclusion within your overall risk assessment.

### 2. Assess the ERM risk inventory

As discussed above, the list of ERM risks is one of the many sources that may be evaluated during the risk assessment process. Depending on your institution, the volume of ERM risks can be significant, and although management may have already narrowed the results to a "top X list," you should further analyze the key risks based upon perception of criticality to the enterprise. This analysis and prioritization of ERM risks may be based upon objective and subjective factors along with consideration of auditable components, which are outlined below.

Auditable Risk Evaluation - Although an ERM risk may be a top/critical risk, it may not have an easily identifiable audit component. Therefore, in conjunction with the objective/subjective analysis described above, determine whether the risks also contain auditable components. Risks with auditable components should continue to be considered during the ERM risk evaluation.

### 3. Merge the ERM Inventory with the Internal Audit Risk Inventory

In addition to analyzing the ERM risks discussed in #2 above, include the most appropriate ERM areas to the IA risk inventories.

Once the steps noted above are complete, include the risks as one of your sources in your overall risk assessment.

ERM can provide valuable input to an auditor's risk assessment. It can identify patterns/trends that can be compared to other risk assessment results (e.g., management conversations, current events, etc.), and provide for feedback that is important to internal audit's risk scoring process and final results.

# APPENDIX A

## RISK UNIVERSE REGISTER

Purpose: To provide a list of auditable areas to consider in audit planning.

Sources: ACUA's Risk Dictionary, Areas Identified by University System of Maryland, Emory University, State University of New York System Administration, Saint Joseph's University and Strayer University

| **Risk Universe Register** |
|---|
| |
| **A. Asset and Risk Management** |
| Emergency Preparedness |
| Environmental Health and Safety |
| Foundations |
| Endowment & Development |
| |
| **B. Auxiliary and Service Departments** |
| Auxiliary Services |
| Bookstore |
| Campus Recreation Services |
| Children/Child Care Centers |
| Housing and Residence Life |
| Intercollegiate Athletics - (NCAA) |
| Jeanne Clery Act Compliance |
| Marketing and Call Center |
| Marketing and Communication |
| Marketing Media Relations |
| Parking and Transportation Services |
| Police Department |
| Recreation Center/Fitness |
| Student Residency |
| Transportation Services |
| Youth Camps and Related Programs |
| Campus Operations |
| Auxiliary Enterprises Administration |
| Service Centers - Auxiliary |
| Special Events Center |
| |
| **C. Financial Management** |
| Accounts Payable |
| Bursar's Office |
| Capital Equipment |

| |
|---|
| Cash Controls |
| Department of Business Services |
| Payroll |
| President/Executive Discretionary Spending |
| Stipend Payments |
| Student Receivables |
| UBIT Compliance |
| Accounting |
| Accounts Receivable |
| Capital Asset Depreciation |
| Cash Handling |
| Cash Management |
| Closing Process |
| Expenses |
| Financial Mgt Operations |
| Financial Reporting |
| Revenue |
| |
| **D. Governance and Leadership** |
| Governance and Leadership |
| Internal Audit |
| Legal |
| Strategic Financial Mgt |
| Institutional Compliance |
| |
| **E. Hospitals and Patient Care** |
| Charge Capture & Collection |
| Patient Care |
| Hospital Building & Facilities |
| Hospital Equipment & Supplies |
| Hospital Human Resources |
| Hospital General |
| Patient Information |
| Compliance |
| |
| **F. Information Technology** |
| IT/IS Security |
| Office of Technology-Intellectual Property |
| IT Security Policy Development & Maintenance |
| IT Security Standards Compliance |
| Logical Security IT/IS Systems - Dining Services *CISO |

| |
|---|
| Logical Security IT/IS Systems - Department Transportation *CISO |
| Managing/Securing PII |
| Network Vulnerability (Network Security) |
| Wireless Network Security |
| KUALI Security |
| Database Security |
| Handheld & PDAs (Mobile Devices) |
| Email |
| Black Board (Other Learning Systems)* (CIO Input) |
| Disaster Recovery |
| Change Management |
| Identity & Access Management |
| IT Admin Support |
| IT Customer Service |
| IT Daily Operations |
| IT Development & Research |
| IT Strategic Planning & Governance |
| IT Compliance |
| |
| **G. Instruction and Academic Support** |
| Academic Administration |
| Academic Records Management |
| Academic Reporting |
| Academic Support and Administration |
| Institute for International Programs |
| International Programs - Education Abroad |
| International Programs - Overseas Operations |
| Study Abroad Programs |
| Academic IT |
| Academic Personnel Administration |
| Courses & Curriculum Development |
| Instruction |
| |
| **H. Medical Center** |
| Hospital Human Resources |
| Patient Information |
| Medical Center General |
| Medical Faculty & Staff |
| |
| **I. Plant Operations and Maintenance** |
| Building and Landscape Services |

| |
|---|
| Capital Construction |
| Custodial Services |
| Facilities Operation |
| Building Maintenance |
| Major Repair & Renovation |
| Motor Pool |
| Physical Plant Administration |
| Utilities |
| |
| **J. Purchasing and Warehousing** |
| Contract Management |
| Inventory Management |
| Procurement |
| Purchase Card |
| |
| **K. Research and Development** |
| Grant Accounting Sponsored Research |
| Grants and Compliance |
| Venture Creation & Entrepreneurship/Intellectual Property |
| Conflict of Interest |
| Animal Research |
| Compliance-Research |
| Facilities & Equipment-Research |
| Financial Fraud - Research |
| Human Subjects Research |
| Intellectual Property/Technology Transfers |
| Pre-Award & Award Acceptance |
| Research Administration |
| Research Financial |
| Research Quality |
| Safety-Research |
| Security-Research |
| Trademark Licensing |
| Export Controls |
| Conflict of Interest |
| |
| **L. School of Medicine** |
| Dental School |
| Department of Psychiatry |
| School of Medicine |
| School of Medicine Dean Discretionary |

| |
|---|
| School of Nursing |
| School of Pharmacy |
| School of Public Health |
| Patient Care |
| Medical Education |
| Clinical Revenue |
| Research |
| Compliance |
| |
| **M. Student Services** |
| Admissions and Enrollment Management |
| Counseling Services |
| Debit/One Card-Student Card |
| Dining Services |
| Financial Aid |
| Health Center/Health Counseling Services |
| Registration |
| Student Judicial Affairs |
| Student Services Administration |
| Title IV / Financial Aid Compliance |
| Enrollment Management |
| Student Centers & Activities |
| |
| **N. University Relations and Alumni Affairs** |
| External Services |
| Stakeholder Relations |
| |
| **O. Human Resource Development** |
| Adjunct Faculty Human Resources |
| Faculty Human Resources |
| Human Resources |
| |
| **P. Colleges/Schools/Departments** *(These audits can encompass multiple risk areas)* |
| Civil Environmental Engineering- |
| College of Education |
| College of Journalism |
| Colleges & Schools: College of Computer, Math & Natural Sciences |
| Colleges and Schools: College of Education |
| Colleges and Schools: College of Information Studies |
| Colleges and Schools: School of Public Policy |

| |
|---|
| Colleges and Schools: College of Behavioral & Social Sciences |
| Graduate School |
| Library Audit |
| Performing Arts |
| School of Engineering Departmental |
| School of Law |
| School of Social Work |
| Dental School |
| Department of Psychiatry |
| School of Medicine |
| School of Medicine Dean Discretionary |
| School of Nursing |
| School of Pharmacy |
| School of Public Health |
| Centers and Institutes |

# APPENDIX B

## EXAMPLE SCORING MATRIX

Purpose: To provide some examples of risk scoring templates.

*Example 1 – Basic*

| | Internal Audit Risk Assessment Determination of Auditable Entities' Risk Scores | | | | | |
|---|---|---|---|---|---|---|
| | Auditable Entities and Risk Areas are Comprised from the Following:<br>*ACUA Risk Dictionary<br>*Industry Events and Activities<br>*Management Discussion and Feedback | | | | | |
| Risk Number | **Risk Areas for Annual Audit Consideration/Inclusion** | A. Operational | B. Financial | C. Compliance | D. Health & Safety | Risk Assessment |
| 1 | Health Services | 5 | 5 | 5 | 5 | 20 |
| 2 | Office of Legislative Audit Follow Up | 5 | 5 | 5 | 3 | 18 |
| 3 | Cash Controls | 5 | 5 | 5 | 2 | 17 |
| 4 | Clery | 3 | 5 | 5 | 5 | 18 |
| 5 | Emergency Preparedness | 3 | 5 | 5 | 5 | 18 |
| 6 | Foundation | 5 | 5 | 5 | 2 | 17 |
| 7 | Youth Programs | 4 | 4 | 5 | 5 | 18 |
| 8 | University Debit Card | 5 | 5 | 3 | 2 | 15 |
| 9 | NCAA Intercollegiate Athletics | 5 | 4 | 5 | 3 | 17 |
| 10 | Purchase Card | 5 | 5 | 4 | 2 | 16 |
| 11 | Procurement | 5 | 5 | 4 | 2 | 16 |
| 12 | Financial Aid | 4 | 5 | 5 | 2 | 16 |

*Example 2 – More Complex*

| Risk Number | Risk Area | Risk Factor Weight | 10% | 10% | 15% | 5% | 5% | 5% | 15% | 10% | 10% | 15% | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Risk Factor | A. Health and Safety | B. Financial Impact | C. Public Image and Reputation | D. Outside Influence | E. Strategic Risks | F. Volume/Size | G. Change | H. Complexity | I. IT and Systems Risk | J. ERM Results | Total Risk | Weighted Risk Score |
| 1 | Cash Controls/ Student Accounts (Includes Travel, Advances, Petty Cash, Uncashed Checks) | | 0 | 5 | 5 | 3 | 3 | 5 | 3 | 1 | 5 | 3 | 33 | 3.30 |
| 2 | Intercollegiate Athletics (NCAA) | | 3 | 2 | 5 | 5 | 3 | 3 | 0 | 5 | 3 | 5 | 34 | 3.55 |

*Example 3 – IT/IS Security*

| | Internal Audit Risk Assessment Determination of Auditable Entities' Risk Scores | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **IT/IS Risk Assessment** | | | | | | | | | |
| Risk Number | **Risk Areas - Auditable IT/IS Components (Source - EDUCAUSE- Security Surveys - University Security Group)** | A. Strategic Planning | B. Operational | C. Financial | D. Compliance | E. Reputation | F. Availability | G. Integrity | H. Confidentiality | Risk Score |
| 1 | Network Vulnerability (Network Security) | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 39 |
| 2 | IT Security Policy Development & Maintenance | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 40 |
| 3 | Wireless Network Security | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 39 |
| 4 | Personally Identifiable Information | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 39 |
| 5 | Database Security | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 39 |
| 6 | Disaster Recovery | 5 | 5 | 5 | 3 | 4 | 5 | 3 | 3 | 33 |
| 7 | Identity & Access Management | 2 | 4 | 2 | 5 | 5 | 5 | 5 | 5 | 33 |
| 8 | Data Privacy | 2 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 33 |
| 9 | Change Management | 3 | 5 | 3 | 3 | 3 | 5 | 5 | 5 | 32 |
| 10 | Environmental & Physical Security | 3 | 4 | 3 | 3 | 2 | 5 | 3 | 3 | 26 |
| 11 | Incident Response | 5 | 5 | 2 | 2 | 5 | 5 | 2 | 2 | 28 |
| 12 | P2P Security (Peer-to-peer (P2P) file sharing) | 2 | 3 | 4 | 4 | 4 | 4 | 1 | 2 | 24 |
| 13 | Spyware/Malware | 2 | 4 | 4 | 2 | 3 | 3 | 3 | 3 | 24 |
| 14 | Aging Hardware (Technology) | 4 | 4 | 2 | 2 | 2 | 4 | 3 | 3 | 24 |
| 15 | IT Staffing | 5 | 5 | 2 | 2 | 1 | 3 | 2 | 2 | 22 |
| 16 | Patch Management | 5 | 5 | 1 | 1 | 1 | 5 | 1 | 1 | 20 |
| 17 | PBX Security | 2 | 2 | 2 | 1 | 1 | 2 | 1 | 1 | 12 |
| 18 | Handheld & PDAs | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 10 |
| 19 | Spam | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 9 |

# APPENDIX C

## RISK ASSESSMENT SURVEY QUESTIONS

Purpose: To provide examples of survey questions from survey responses from ACUA leaders charged with audit planning.

**A** Audit Universe Questions

1 Does the Department currently have grants?

2 Does the Department/Area have a Petty Cash Fund? If so, what is the amount and purpose of the fund?

3 Current Number of FTEs employed in the department.

4 Last Three Years Total Budget Amount (All Accounts).

5 Revenue/Assets - Does the Department/Area have revenues (Funds or receipts not provided as part of the budget appropriation process -cash, check, credit card, etc.)? If so, please give the approximate yearly amount.

6 Does the Department/Area have inventories of any kind? If so, please describe the inventory in general terms and give an approximate value.

7 Do you have any departmental inventory (not fixed assets or equipment) or specialized inventory such as controlled substances, hazardous wastes, or precious metals?

_____ 1. Inventories are valued at low dollar amounts.

_____ 2. Inventories are at relatively moderate dollar amounts.

_____ 3. Inventories are valued at high dollar amounts or include specialized items, such

8 Are there any units, areas or processes of which an audit would be beneficial during this coming year? Include a brief description of the risks that should be considered for review.

9 To what extent does your department handle cash?

_____ 1. Does not handle any cash, checks, or credit card payments.

_____ 2. There is limited activity or potential for access to them.

_____ 3. Significant amount of handling of cash, checks, and credit card payments.

**B** Risk Assessment Questions

1 If your department had either an internal audit or was part of the external audit, what kind of findings or exceptions were there?

_____ 1. Only minor exceptions were noted in the department's activities and they have been addressed.

_____ 2. Some minor to moderate exceptions have occurred causing some control concerns.

_____ 3. Significant exceptions have been revealed during past audits.

2 This responsibility center has been audited or reviewed within the past three years.

3 Audits or reviews conducted within the last three years have noted significant findings or other problems. (Please identify any significant findings and their resolution in the 'Comments' section.)

4 All findings or problems identified in audits or reviews were addressed in a timely manner.

5 Has your Department experienced rapid or unexpected growth in services provided during the past fiscal year that had a significant impact on your department's operations? If yes, please explain.

6 Indicate the whether there has been growth in your department in number of activities or budget during the past 12 months.

_____ 1. The unit has experienced no growth or has shrunk in size.

_____ 2. The unit has experienced less than 10% growth.

_____ 3. The unit has experienced more than 10% growth.

7 Department Losses - Has your Department had any material losses in funding during the past fiscal year? If yes, please explain the effect this has had on your operations.

8 To what degree can management of this department supersede the policies established for this particular activity?

_____ 1. Complete inability to circumvent controls.

_____ 2. Capability to override some controls without detection.

_____ 3. Capability to override the majority or all of the controls without detection.

9 Please indicate the status of training in your department?

_____ 1. Training is provided at least annually to all applicable employees.

_____ 2. Some training is being provided to applicable employees.

_____ 3. Very little training is being provided.

10 Do you routinely have communication with outside parties such as: legislators, news media, citizen groups, or agency personnel?

_____ 1. Outside parties have shown no or very little interest in the area

_____ 2. Outside parties have shown a moderate interest in the area.

_____ 3. Outside parties have shown a major interest in the area.

11 This responsibility center has in writing a clear, concise mission/vision statement.

12 Does your Department have written policies and procedures for the initiation and processing of transactions by employees?

13 In regard to departmental policies and detailed procedures to support the policies, indicate whether.

_____ 1. Policies have been in place for over three years, with no major changes made.

_____ 2. Policies are in place; however, employees are not always familiar with them.

_____ 3. No written policies are in place.

14 Policies and procedures governing this responsibility center are documented, kept current and readily available to all employees.

15 New and revised policies and procedures are communicated to all employees within the responsibility center.

16 The organization chart for this responsibility center is current and accurate.

17 Delegations of authority for specific areas of responsibility are periodically reviewed, updated, and made available to all employees within the responsibility center.

18 Management and supervisory reviews of responsibility center processes and procedures are performed routinely.

19 Responsibility is divided so that no single employee controls all phases of a transaction.

20 If the responsibility center's organizational structure requires individual employees to control all phases of a transaction, please describe any compensating controls in the 'Comments' section.

21 A budget planning process exists and is integrated with the goals and objectives of this responsibility center.

22 Budget allocations are communicated in writing to all relevant employees in this responsibility center.

23 Expenditure reports are used by appropriate staff within the responsibility center to monitor expenditures and account accuracy on a regular basis.

24 Credential verification and reference checks are made of selected job applicants (excluding students).

25 This responsibility center provides some form of orientation for new employees.

26 Each employee in this responsibility center has a current position description and performance program that clearly defines the duties for which he or she is responsible.

27 All employee performance programs and appraisals have been completed and submitted to Human Resources within the last twelve months.

28 Timesheets and monthly leave records are reviewed for accuracy and compliance by the appropriate supervisor.

29 Time and attendance records are up to date and on file for all employees in this responsibility center.

30 Employee turnover is a significant concern in this responsibility center.

31 This responsibility center has established backup plans for sudden or significant changes in personnel.

32 This responsibility center has developed a succession plan.

33 This responsibility center has developed a business continuity plan.

34 This responsibility center has developed an information technology disaster recovery plan.

35 Has your Department incurred any fraud or misappropriations the past fiscal year?

36 Have there been any instances of fraud, computer abuse, or data loss for this department?

37 Are there significant laws/regulations/policies where a review of the program for compliance would provide comfort?

38 Significant Changes - Law/Regulation - Has your Department been impacted by new regulations during the past fiscal year that required significant changes in your department's operations? If yes, please explain.

39 Has your Department had any changes in key personnel/ positions in your organization during the past fiscal year? If yes, please explain.

40 Have there been any significant changes in staff size, funding, functions, systems, key positions and/or responsibilities of the department which might create problems?

_____ 1. No turnover in key management or staff.

_____ 2. Limited turnover in key management or staff.

_____ 3. Major turnover in key management or staff.

41 Significant Changes - Process - Has your Department implemented any new systems, programs, or processes during the past fiscal year that have a significant impact on your department's operations? If yes, please explain.

42 Have there been any recent significant changes or are there any anticipated changes for fiscal year 2016 (e.g., system implementation, organizational structure)?

43 What level of impact does Information Technology (IT) have on your department?

_____ 1. There have been no new IT changes during the past 12 months.

_____ 2. Some changes have been made to the IT environment.

_____ 3. The IT environment has changed or been replaced.

44 What are the major business risks and/or issues facing your area(s)?

45 What are the key risks (operational, financial, or technical) that would threaten the achievement of your goals and objectives?

46 Are there any other comments or information you would like to share or is there anything I thought I should have asked but did not?

## C Self-Assessment Questions

1 Key personnel in the responsibility center understand the budget planning and development process.

2 Key personnel are aware of federal, state, and university regulations and policies as they relate to the responsibility center (i.e., ADA, Affirmative Action, discrimination, sexual harassment, HIPAA, FERPA, etc.).

3 State employees are familiar with code of ethics/ethics standards encouraging ethical behavior and preventing conflicts of interest in state government.

4 Do you have concerns regarding:

a. Potentially fraudulent activity?

# APPENDIX D

## ACUA SURVEY RESULTS "OTHER" – WHAT RISK FACTORS DO YOU USE WHEN SCORING RISK

- We rank risks only based on impact and probability,
- While not using a formal risk scoring matrix, we do use the above categories in discussions,
- Likelihood,
- Compliance with regulations,
- Reg/Legal Impact, Quality of Internal Controls,
- Opportunity for Fraud/Waste/Abuse,
- Fraud,
- While all above checked factors are considered, there is no separate scoring for each factor,
- Whistleblower information,
- Compliance with risk rating being based on results of noncompliance and complexity of requirements,
- Operational with risk rating being based on criticality to daily operations,
- Likelihood, Impact, Velocity,
- We identify key business objectives and related risks,
- Quantitative risk scores are assigned based on financial and operational data that is mined from our system,
- Compliance requirements,
- Research and Compliance Risks; Fraud Risks,
- Compliance Risk,
- Known issues, Legal/Regulatory landscape, Fraud risks, Overall Internal Control Environment maturity/quality, etc.,
- Compliance,
- I combine and have five topics strategic, operational, compliance financial and stakeholder risks,
- Compliance Requirements (health and safety is one),
- Audit Required by Law or Regulation, Potential for Fraud or Non-compliance with Laws & Regulations, Management Interest,
- COSO RISKS,
- Legal and academic risks,
- Federal, State, and local compliance requirements,
- Operational risks and (ii) Regulatory compliance risks,
- Length of time since last audit with regard to audit coverage,
- Regulations, liquidity, budget deviations, executive assessment,
- Compliance risk,
- Compliance Requirements,
- Length of Time and Results of Prior Audit are combined as one factor,
- Regulatory compliance requirements,
- Compliance (Regulatory); Fraud, Waste, Abuse, Error,
- Likelihood of an issue (Which brings in Change, complexity, etc.),
- Compliance.