AUECO
ASSOCIATION OF UNIVERSITY EXPORT CONTROL OFFICERS

Guidance Paper

Risk Assessment

Issue date:
October 2016

Introduction

Risk assessments (RA) are a valuable tool to proactively determine what concerns or risks are present (and need to be addressed) within a compliance program. Depending upon the type of assessment tool used, an RA can be used to:

1. Identify risks.
2. Assess the severity of a given risk.
3. Assess the likelihood of occurrence for a particular issue.
4. Determine program priorities.
5. Develop action (mitigation) plans to address risk.

RAs can be used to review the compliance risk for an entire campus, or smaller portions of a campus, such as colleges, departments or institutes. They also can be used to assess specific activities on campus, such as certain types of research, international travel and visa beneficiaries.

RAs are a key tool in the arsenal of a compliance manager to justify priorities, resourcing (staffing, costs and education) and activities to organizational leadership. Start-up programs can use RAs to determine what compliance risks are present and what needs to be addressed first on their campuses, while a more mature program may use RAs to determine the status or "health" of their program by assessing success metrics (have all key risks been addressed) or by identification of gaps or other program failure points. In either case, conducting periodic RAs (annually or biannually) is a key element in determining the status (well-being) of any compliance program.

What Is A Risk Assessment?

A risk assessment is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking (Oxford Dictionary). They can be used in many disciplines to assess the relative risk of diverse concerns. Examples are:

- Investing – The potential to lose a significant portion or all of your investment.
- Safety – The potential for an issue to cause harm to people or equipment.
- Business – The likelihood of a project being completed on time and on budget.
- Health – The likelihood that treatment of a certain disease could cause an unwanted event.
- Research – The chance that a research project will not meet its objectives.

In the regulatory/compliance arena, risk typically presents itself as non-compliance. Depending on the nature of the non-compliance, the outcome may result in fines, penalties, jail time, additional costs (i.e., hiring consultants or additional staff), audits, new or changed processes, and/or work stoppages. In many instances, the severity of these "penalties" may dictate the risk tolerance of an organization. Issues that result in minor penalties may embolden an organization to assume more risk as the financial or operational impacts will be minor on the organization (even if they get caught). Infractions that result in significant fines and penalties tend to make organizations more risk averse.

Every institution should actively determine its institutional risk tolerance levels, which may vary from one compliance area to another, to help inform rational decision making in the operation and enforcement of its compliance programs. In addition, as risk tolerance may change over the years depending on multiple factors, including the type of research activities in which a university engages and what relative level of compliance (track record) has been in a given area, the ongoing evaluation of institutional risk tolerance should be part of the regular analysis of any institutional compliance program. Conducting a periodic RA of your export compliance program

is an excellent means of gauging the current risk tolerance of your university and your export compliance staff.

The RA process includes the identification, evaluation and estimation of the various compliance concerns (risks) that could present themselves during the daily operations of your export compliance program. RAs may be qualitative (subjective evaluations of risk), quantitative (statistical evaluation of risk) or a combination thereof. There is no set way of completing a risk assessment and each institution should find a process that suits the nature of the institution. Notwithstanding the need for individualization of approaches, included with this Guidance Paper are some examples of sample assessment tools that can be used as starting points for any institutional RA (Sample Assessment Tools available online as a separate document).

The principal steps in conducting a RA including the following:

1. **Identification of the Issues** – Identify the issues or activities with which you are concerned. For export compliance, these issues may include:
    a. Areas of research, such as military, satellites, select agents, encryption, computers and infrared sensors;
    b. Foreign Nationals (FNs) on-site (ex. FNs working in research labs);
    c. Foreign students and visitors;
    d. International shipping;
    e. International travel;
    f. Research collaborations;
    g. Purchasing (what you purchase from others);
    h. E-Commerce considerations (what others purchase or download from you); and,
    i. Non-disclosure agreements.
2. **Impact (Severity) Assessment** – For the issues above (or for other issues identified as unique to your institution), an assessment of the impact/severity of non-compliance events should be conducted. For example, the failure to obtain an export license for an international shipment of a Select Agent is an event of non-compliance likely to impact current operations (fines/penalties/shipping holds) as well as future export processes (license scrutiny/enforcement actions/reputational harm).
3. **Likelihood (Probability) Assessment** – For each issue above, complete an assessment of the probability of that issue both occurring **and** resulting in the impact noted.
4. **Level of Risk** – Generate an institution-specific expression of comparative risk determined by a juxtaposition of the impact determination in relation to the likelihood determination. Level of risk may be indicated either subjectively (using terminology such as “Minor”, “Moderate” or “Major”) or objectively (numerical or hierarchical ordering).
5. **Priority** – The priority of the issues may be simply a reflection of the risk assigned to the issues. For subjectively scored risks, a major risk takes precedence over a moderate. When numerically scored, higher scores are generally of greater priority than lower scores.
6. **Mitigation** – The nature of the controls (mitigations or action plans) for each issue should match the risk of the issue. A minor issue may not require any controls, whereas a major issue may require the development of a review process, screening form, tracking database and training.

Focus and Type of Institutional Risk Assessments

Any RAs undertaken at your institution will first need to be tailored to the specific circumstances which are in existence at the time of the RA. While the suggestions and examples in this document are designed to facilitate the conduct of an Export Compliance RA at many U.S. institutions of higher education, no prepared forms can ever prepare you or your institution 100% for conducting a RA. The following discussion of the focus and types of an Institutional Risk Assessment may, however, help you to plan, develop and tailor the appropriate direction for conducting a successful assessment.

A. Focus (Scope) of an Institutional Risk Assessment:

Determining the necessary focus and scope of a RA involves more than a condensing of an evaluation or assessment tool to a particular content area of interest or concern. It also requires strategic planning to identify the appropriate level of focus and/or scope of the assessment itself. This process must also include a consideration of the team included in conducting any level of RA. Due to inherent bias and human error, AUECO recommends that a cross-campus team conduct the RA together in an attempt to minimize these negative effects. The following examples are not an exhaustive representation of the potential focuses/scopes of an assessment of institutional export compliance, but these examples can be considered as traditional entry points into the evaluation of institutional export compliance risks. Those considering undertaking an institutional RA for export compliance purposes should and are encouraged to use multiple approaches and even to mingle the approaches, as needed, to meet the unique evaluation needs of their own institution.

1. **Strategic Risk Assessments** – "*Broad Institutional Analysis*"– The evaluation of the intersection of the institutional strategic planning, vision and mission with its obligation in an increasingly global educational and research environment may help to identify programmatic issues or concerns with current or proposed export compliance efforts. Identification of these intersection points may also help to sell and/or justify export compliance operations, programs, procedures or materials which fit within the institution's "Big Picture" strategic plan. Working with Senior Administration to make concrete connections between existing or desired compliance efforts will help create the synergy necessary to drive change or encourage institutional buy-in to export compliance efforts.
2. **Operational Level Assessments** – "*Where The Rubber Hits The Road*" – While it is often critical to complete the Strategic Risk Assessment to focus on how the export compliance program fits within the mold of the overarching strategic plan, vision and mission of the organization, the devil is often in the details. The Operational level assessment focuses on an evaluation of the potential harms which might occur and/or the benefits to be obtained from either the failures or the successes of the existing export compliance programs and efforts. This RA requires a deeper dive into the operational realities of the institution, by looking at the internal processes, people and systems as they relate to internal or external export compliance triggers. Operational level RAs are often the approach utilized for any required regulatory assessments or reviews, since the operational level assessment is generally the most concrete and well defined assessment approach.
3. **Compliance Program Risk Assessment** – "*Seeking to Meet Our Compliance Burdens*" – Conducting an assessment with a focus on the compliance program itself is the most uncomfortable approach for the compliance team. This type of RA requires a look into the current standards and best practices of the institution in relation to the current regulatory and legal framework. Questions often asked as part of a Compliance Program RA include – "Is our program designed to meet the legal/regulatory requirements or the unique needs of the institution", and "Is there a conflict between those two goals?" Evaluating current institutional risk in relation to the actual compliance burdens under applicable law, regulation and policy may help to reorient the program in a way that serves to narrow the spread between institutional practice and regulatory requirements. A Compliance Program RA will require direct and substantial involvement of the compliance team in consultation with representatives from other operational staff to document the actual impact costs of the implementation of current compliance program efforts.
4. **Internal Audit Assessments** – "*Stress Testing the Performance of the Program*" – The final focus approach discussed here is that of conducting an internal risk audit of the program itself. This is often the most immediately proactive, as the successful completion of the initial internal audit of the compliance function will often result in a formalized response plan. In an internal audit assessment, the institutional monitors will consider the impact of current programs against the specific interests of the customer bases and institutional business interests. The result of this focus approach is most often an action plan to encourage the reformulation of programs, processes and procedures to meet the identified strategic goals

and needs of the entity. If done correctly, an internal audit assessment of an institution's compliance efforts can create great momentum for necessary change in the visualization and management of compliance related risks.

B. Types of Risk Assessments:

In addition to the strategic consideration of the focus/scope of the RA, it is critical to identify the type and depth of information to be evaluated and then structure the RA process/tools around that information. As with the discussion of focus/scope above, the following list of general types of RAs, while not exhaustive, may help compliance staff to better prepare for the actual performance of the RA.

1. **Baseline Risk Assessments** – A Baseline RA is designed to set the risk threshold and to identify a risk profile. In other words, it is designed to identify the types and extent of risk. It can also be used as a preliminary ordering of criticality of risk. Terms of art often used in the baseline risk assessment process include benchmarking and "big picture" reviews. The Baseline RA is best utilized to "hone in" on areas for additional review or assessment. While flexible enough to be used in both targeted and comprehensive evaluations, the Baseline RA often lacks sufficient detail to drive performance changes by itself. The successful completion of a Baseline RA should produce the following types of outcomes:
    a. A clear description of the institutional risk profile or risk profiles; and,
    b. A clear description of the means and methodology utilized in conducting the Baseline RA, to facilitate appropriate use and potential future extension or improvement of the Baseline RA.
2. **Issue-Based Assessment** – An Issue-Based RA is used to conduct a more detailed investigation into a specific issue or focus area in order to develop a concrete action plan for mitigation of risk and/or to otherwise respond to specific concerns identified in the institutional risk profile. This type of RA is often teamed with the operational focus approach to identify current program strengths/weaknesses and to propose improved policies, processes, and/or procedures. Issue-Based RAs tend to be most successful when kept narrowly tailored to the identified risk profile concerns that are the genesis of the RA. This RA type is often a direct follow up to an initial Baseline RA and helps to give additional form to the resultant risk profile. The Issue-Based RA is also a common result from either "near miss" scenarios and/or actual system failures. While conducting a wide-ranging Issue-Based RA can be accomplished, it often gets derailed by the complex details and fails to meet key deadlines and action items due to the constantly changing nature of both the ongoing institutional compliance efforts as well as the underlying regulatory demands/burdens. The desired outcome for an Issue-Based RA is generally a clear and concise recommendation to management for the development and/or implementation of specific action plans designed to close the gap in existing policies, processes or procedures.
3. **Continuous Risk Assessment** – As the name suggests, the Continuous RA is used for the ongoing evaluation of program operations against fixed and identified standards for performance. It is an extremely important and valuable part of any RA process, and one that is often overlooked due to the draining nature of the RA process as a whole. The Continuous RA serves as the day-to-day program evaluation, and should be used to encourage growth and maturation of the compliance program itself. The focus here is often on hazard awareness and remediation. The Continuous RA may use forms, checklists and automated systems to help track and document program efficiency, especially as it relates to the mitigation and remediation of any direct impacts on the institutional risk profile established as part of the Baseline RA. It is often the responsibility of front-line compliance managers to be constantly evaluating and encouraging improvements as part of a Continuous RA process. Common buzzwords in the Continuous RA process include audit, inspection, recalibration, refocusing, and stress-testing. While Continuous RAs may be used for long-term evaluation of risk profiles and risk management, using an agile approach to project management is often the best way to encourage ongoing program growth, development and improvement. The outcome of the Continuous RA is typically the incremental change

or improvement of the operational tools used to meet the compliance needs of the organization.

Guidance paper authors:
Scot Allen
Colorado State University

Thomas Demke
University of Wisconsin – Madison

Wayne Mowery
Pennsylvania State University

Others recognized for direct contributions:
David Brady
Virginia Polytechnic Institute and State University

Elizabeth Peloso
University of Pennsylvania

Gretta Rowold
University of Oklahoma