CONDUCTING EFFECTIVE ENTERPRISE RISK ASSESSMENTS IN NOT-FOR-PROFIT ORGANIZATIONS

It is recommended that organizations conducting any type of risk assessment consult with legal counsel before, during and after the process. It is important to understand, however, that even with a lawyer involved in the process only their legal advice and communications for purposes of obtaining legal advice are protected from disclosure to third parties under the attorney-client privilege doctrine. Risk assessment processes and outcomes may be viewed as business advice and decisions rather than legal, which means they will not be protected from disclosure even if a lawyer is involved in the process.

The information in this document is intended to be a general overview of effective, Enterprise Risk Assessment, and not legal advice for any specific organization or situation. Organizations are advised to use this document as a guide and a tool, in consultation with organizational leadership and legal counsel to customize for the specific needs of the organization.

TABLE OF CONTENTS

INTRODUCTION

Risk Assessment is an inherently customized task; the reasons, process and outcome, and even who will conduct it, will vary greatly from one organization to the next. In order for the risk assessment to be effective, each organization must be thoughtful about its own specific operations and culture. Thus, this document is intended as a guide for the creation of a customized Enterprise Risk Assessment tool, not a Risk Assessment tool itself.

This introduction provides a general overview of Risk Management, Risk Assessment, and the key terminology used in the Risk Assessment process.

What is Risk Management?

Risk Management is defined as a process that helps an organization plan for the possibility that events may cause it harm, focusing specifically on risk associated with board members and volunteers, staff, programs and events, services offered, operations, technology and financial management. Managing risk guides organizations to effective decision-making consistent with the organization's mission, strategic priorities and risk tolerance level. Understanding risk does not always lead an organization to avoid that risk, but allows the organization and its leadership to prepare better for the potential outcomes of undertaking risky ventures.

Many functions within organizations manage risk effectively within their function or isolated tasks of their function. Enterprise Risk Management ("ERM") expands the scope of potential risk to include anything that could prevent the organization from achieving its mission and strategic objectives, looking at the organization as a whole rather than select functions or tasks. ERM enables non-profit leaders to see whether strategic objectives are being met while identifying and managing internal and external risks across the organization. By analyzing the vulnerability of the organization, leaders are able to link related risks to the organization's key initiatives and mitigate the potential impact of these risks.

In the simplest possible terms, Risk Assessment is a tool that determines the processes, procedures and functions of an organization that present risk to the strategic, financial, operational or reputational viability of the organization while assessing the potential impact of each risk, and the sufficiency of the organization's efforts to mitigate that risk. Risks can be ***inherent*** (i.e. simply providing a service poses the risk that someone will make a mistake) or ***external*** (i.e. a hurricane that floods a community-based program location).

Many organizations approach Enterprise Risk Assessment as a new and daunting task. In reality, however, most organizations already have processes in place to mitigate known risks. For example:

- Organizations that conduct background checks on potential new hires have recognized the risks associated with hiring individuals who do not have the requisite licenses or experience to provide services or, perhaps, have a criminal conviction disqualifying them from a particular job.
- Organizations obtain insurance to guard against the risk of service interruption associated with unavoidable events, such as natural disasters.
- Organizations separate responsibilities around handling money – one employee records the income received while another employee deposits the income and, in some cases, a third employee reconciles their records. This segregation of duties guards against the risk of one employee having the ability to divert the organization's revenue.

Enterprise Risk Assessment and ERM provide the rationale for these safeguards, as well as a structure for the risk management processes and procedures that most organizations are already doing. Moreover, it allows organizations to assess periodically whether existing risk management and mitigation resources are being applied appropriately based on the assessment of each risk's relative severity, likelihood and speed of impact.

This means that organizations conduct Enterprise Risk Assessment so they can identify, assess and mitigate risks within the organization. Steps for conducting Risk Assessments will be discussed below. For now, we will work with the very broad characterization that ***risk assessments are tools for determining where an organization has risks, the potential impact of those risks and whether current efforts to mitigate those risks are sufficient***.

Risk Assessment Terminology

Before embarking on a study of Risk Assessment, it is important to set the scope for the discussion, including the definition of several key terms. While these are all different terms, individuals often use the terms interchangeably; any time someone starts a discussion of risk assessment generally, it is a good idea to make sure everyone is using the terms in the same way.

For purposes of this Guide, the following definitions apply:

- "*Risk*" is anything that can prevent the organization from achieving its objectives.
- "*Risk Management*" is the overall concept of addressing risk. This includes everything an organization does to address risk, which

could include assessment, evaluation, mitigation, insurance, investigation, remediation, etc.

- "*Risk Assessment*" is a Risk Management tool. It helps an organization assess the levels of risk in various areas of the organization as well as current efforts to mitigate that risk, in order to determine whether additional mitigation efforts are needed, or resources should be reallocated.
- While Risk Assessment and Risk Management are activities that can be focused on one or more discreet areas of the business, "*Enterprise Risk Assessment*" and "*Enterprise Risk Management*" involve the assessment and management of risk across an entire organization. Individual functions may carry out their own Risk Management and/or Assessment on an ongoing or periodic basis, but these do not replace ERA or ERM which generally are requested by and conducted at the highest level of an organization, and look at risk from an organization-wide perspective rather than within a particular function or task.
- The following terms describe functions within organizations:
    - "***Operations***" refers to the areas of the organization responsible for delivering services;
    - "***Administration***" refers to the functions within an organization that support Operations, such as finance, human resources, information technology, legal, etc.;
    - "***Quality Assurance***" is the function that assesses the quality of the services provided through auditing, monitoring and investigations – this functions sometimes sits within Operations and sometimes is an independent function on its own or within Administration;
    - "***Leadership***" is meant to refer to the individuals who are considered the "executive" level employees of the organization;
    - "***Board***" is the Board of Directors of the organization;
    - "***Volunteer***" refers to anyone who volunteers for the organization, including the members of the Board;
    - "***Donor***" refers to individuals and organizations who donate financially to the organization;
    - "***Funding Source***" includes individuals and organizations who provide funding for the organization's services, and can include Donors, government agencies, third-party payors (i.e. insurance, Medicaid), foundations, trusts, etc.

While it may be stating the obvious, it is important to remember that issues that seem to be of critical concern when looking only at one area of an organization may not be assessed to be as important when compared to risks identified in other functions in an enterprise-wide risk assessment.

While function-specific risk assessment has its place in an organization's risk management strategy, only ERA allows an organization to ensure it is allocating resources appropriately throughout the organization. Moreover, the federal government increasingly seeks certification of *Enterprise-wide* risk assessment as a condition for the receipt of federal funds.

For purposes of this Guide, the term Risk Assessment will apply generally to any scope of risk assessment, unless specifically referencing ERA.

Before conducting a Risk Assessment and determining the scope, it is important to understand the ironic truth that conducting a Risk Assessment itself poses some risks.

Risks of Assessing Risk

The fact that conducting a Risk Assessment can present risks does not mean that an organization should not do it. Rather, the organization's leadership needs to plan for the possible risks that simply *doing* a risk assessment may create, and minimize those risks as part of the assessment process.

For example:

- talking to both Board members and employees about risk, especially when it is done for the first time, can create concerns and questions which are best addressed by effective communication underscoring the value of the process and the importance of open and honest participation.
- an organization has to be prepared to address critical, unmitigated risks identified by the assessment. A complete risk assessment, therefore, includes an action plan that explains how the organization plans to address identified risks how the identified risk(s) are acceptable given the organization's mission, strategy and risk appetite.
- organizations may want to engage in activities that have inherent risk in order to meet their strategic goals. Having a strategic plan before conducting a risk assessment can help the organization decide on the strategic priorities where the organization may be willing to have a greater appetite for risk. The organization's willingness to take risks in some areas and not others should be reinforced by the organization's leaders and addressed in the risk assessment process. For example, fundraising campaigns may be designed to be aggressive, which can

offend some potential donors. This is a strategy with potential financial and reputational risk with which a board may be comfortable. Of course, an organization's appetite for taking risks should not be used as a justification to engage in unlawful conduct.

- conducting a Risk Assessment takes time, and existing staff may feel overwhelmed and stressed when asked to participate in the assessment. This is another area where leaders can help with effective communication of the need for the risk assessment and assistance in establishing time management priorities.
- the outcome of a risk assessment may be discoverable in any future litigation or government investigation. This means that, if the organization is defending a legal action or an investigation by a government agency, the risk assessment may become evidence that the organization knew about a particular risk. Some potential strategies for addressing this include privilege, which is discussed in Appendix A.

Despite these risks, conducting a risk assessment and implementing an effective action plan is preferable to ignorance about the risks that exist. Remember – the risks are there whether you learn about them or not, and knowledge is a powerful tool in planning for, preventing and mitigating the effects of adverse events.

WHY CONDUCT RISK ASSESSMENT?

Opportunity to Mitigate

It may seem counterintuitive for an organization to conduct an exercise that essentially looks for risk. It is important to remember, however, that ***the risks are there whether known or not*** – it is better to identify what *could* go wrong and be prepared for it than to be caught off guard. Moreover, assessing risk gives organizations the opportunity to mitigate risk and perhaps prevent an adverse event from occurring, or from causing as much harm as it could have.

Conducting risk assessments also informs decision-making within organizations. Identifying the risks inherent in operational choices, for example, ensures that decisions are made thoughtfully with consideration of potential pitfalls.

Although risks are commonly thought of as threats to an organization, evaluation of risks often creates opportunities. For example, identifying a high risk of losing funding may lead an organization to redirect resources to seek new sources of funding.

Identifying potential risks allows an organization to allocate resources to:

- prevent or reduce the likelihood of inherent risk: that is, risks that exist simply by operating the organization as intended;
- link critical strategies with key risks; and
- mitigate the damage that could be caused by external risks, such as natural disasters or errors by third parties the organization relies on for resources needed to conduct its business.

Ultimately, minimizing the likelihood and impact of risk is a tremendous benefit to any organization.

Risk Mitigation Increases Organization Value

Another reward for effective risk management practices is increasing the value of the organization. Potential strategic partners and funding sources increasingly ask organizations for information not only about finances but also operational compliance and risk mitigation efforts. If given the choice, organizations and individuals prefer to do business with and/or donate funds to organizations that have identified and minimized significant risks.

Thus, there are rewards for effective risk management, what might be called the "carrots." Prepared organizations can respond faster and more effectively, and are more attractive partners for other organizations and funding sources.

Effective Compliance Program

There are, in addition, some "sticks" to go along with these carrots that underscore the reasons for effective risk management. Risk Assessment and effective implementation of the resulting action plan are essential parts of an effective compliance program, which is essential to minimize penalties if an organization is investigated for possible unlawful conduct.

According to several regulatory requirements, organizations must have an effective compliance program, which includes periodic risk assessment. We discuss compliance programs more fully at the end of this article in the section on implementation of an Action Plan following Risk Assessment.

Federal Funding and Reimbursement Requirements

A new HHS/Office of Community Services (OCS) performance standard mandated for designated CSBG eligible Community Action Agencies (CAAs) requires that "[a]n organization-wide comprehensive risk assessment has been

completed in the past 2 years and reported to the governing board." This standard, if assessed to be unmet or uncorrected, may lead to a finding that could interrupt state pass-through funding.[1]

Moreover, any organization that receives funding or reimbursement for services from the federal government is subject to several regulatory requirements. The list of these requirements is long, but the most common involve accurate billing (*e.g.*, False Claims Act), not hiring employees on the System for Award Management list[2] of individuals excluded from providing services to the federal government, and not contracting suppliers who are on the Office of Foreign Assets Control[3] list of suspected terrorist organizations. When any type of organization is found guilty of a federal crime, the judicial system turns to the U.S. Federal Sentencing Guidelines[4] to determine the punishment (i.e. how much to fine the organization). Even without a finding of guilt there is often a type of settlement with the United States Department of Justice ("DOJ") that includes elements from the sentencing guidelines.

WHO SHOULD OWN ENTERPRISE RISK ASSESSMENT?

While both public funding accountability guidelines and best practice standards confirm that organizations conducting ERAs must report results to the Board, there is no mandate stipulating who should lead or manage the assessment process.

In order to ensure accountability and priority of the process, the Board should:

1. formally request the Enterprise Risk Assessment be conducted, including:
    a. requesting the organization's Executive Director/CEO or his/her designee to oversee the conduct of the assessment;
    b. providing a due date for the report;
    c. monitoring progress on the conduct of the assessment;
2. review the report and outcomes;
3. adopt an action plan and monitor implementation;
4. ensure that the assessment and plan are updated at least every two years (more frequently if significant changes in the organization's mission, strategy or service model make the prior assessment irrelevant or outdated).

[1] Because of this requirement, this guide will focus on ERA, which, for designated Community Action Agencies, will need to be conducted at least every two years in order to meet this standard. Nothing in this Guide should prevent an organization's specific functions from conducting their own function-specific risk assessment in addition to the enterprise-wide activity. While the process described in this Guide may be useful for function-specific risk assessment, this Guide does not provide unique guidance for smaller-scope risk assessments.
[2] https://uscontractorregistration.com/
[3] https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fuzzy_logic.aspx
[4] http://www.ussc.gov/guidelines-manual/organizational-guidelines

The Leadership employee who owns the process should then pull together a team to conduct the ERA and oversee the activity to assure timely completion of the assessment. Whether the Leadership employee is part of the team that conducts the risk assessment or serves as an overseer and advisor will depend on the size of the organization and resources available.

WHO SHOULD BE ON THE RISK ASSESSMENT TEAM?

Deciding who should be on the risk assessment team depends in part on many factors, such as adequate or competent staffing resources, financial resources or whether the intent is to conduct an assessment directed by financial auditors or by legal counsel. This is a strategic decision that should be made in a conversation between senior leadership and legal counsel.

Normally, enterprise risk assessment activities include interviews with board members and employees at multiple levels, written surveys and perhaps even focus groups. The individuals who conduct these activities should be at a high enough level to be able to understand, interpret and analyze what is learned, but not so high up that employees are intimidated from speaking openly with them.

To conduct an effective ERA, a cross-functional team of individuals is most effective. With multiple functions providing input into the tools, conducting interviews and assessing the data, different perspectives are integrated into one process. When interviews are conducted, having a team of individuals allows for the recusal of an interviewee's line management whose presence could prevent open dialogue.

Many organizations form a committee to develop risk management programs. Committee members should be included from various segments of the organization, including administration, operations, finance, volunteers, programs/events and development Select board members and the executive director should also be included, at least in an oversight and advisory role if not performing tasks. They represent the voice of the organization's leadership to keep the risk assessment team on track, and ensure alignment with organizational priorities and risk appetite. Moreover, the presence of organizational leadership on the team encourages participation from throughout the organization.

WHEN AND HOW OFTEN TO CONDUCT RISK ASSESSMENT?

Based on the HHS-OCS Federal Performance Monitoring standard, ERA needs to be conducted at least every two years for any Community Action Agency.[5] In addition to this bi-annual ERA process, certain events may come up that make the prior ERA and action plan irrelevant, outdated or otherwise in need of revision. Examples of situations that may occur to necessitate more frequent ERA include:

- at the request or instruction of the Board (public companies due this annually);
- when there is a change in senior leadership;
- when the organization's mission, strategic direction or regulatory requirements change significantly;
- when the organization adds or eliminates a service delivery program;
- when there are significant changes in the demographics or composition of the donors, volunteers or individuals served by the organization; or
- at the end of a routine audit cycle.

Viewing ERA as an "event," however, belies the true nature of a risk assessment. The collection of information might happen only once every two years, but the entire process involves tasks that might take some or all of the two-year cycle to complete. These tasks include, for example:

1. identifying the risks to be analyzed;
2. interviewing key individuals to narrow and focus the list of risks to assess;
3. conducting a survey or focus group (or both) to fully assess each identified risk;
4. reviewing and analyzing the data;
5. creating an action plan to ensure appropriate allocation of resources based on the risk assessment data;
6. implementing the action plan;
7. following up to ensure effective implementation of the action plan.

Once these tasks are completed, it is entirely possible that the time for a new, biennial ERA is approaching. Effective ERA is most effective as an ongoing process rather than an isolated event or task.

[5] Without this mandate, an organization can and should conduct an ERA periodically.

HOW TO CONDUCT RISK ASSESSMENT

The act of conducting an ERA is as much art as it is science because each organization is unique, making its risk profile unique as well. Careful attention to stakeholders, culture, mission, strategic priorities and other specifics must be paid in order for a risk assessment to have value. In fact, without careful consideration of unique characteristics, a risk assessment may do more harm than good.

When identifying risks, it is important to carefully consider the types of risks faced by the organization and to think broadly. Risks can be categorized as either risks to avoid or risks of failure. Some common areas that have a high potential for risk are:

- Strategic Risk
- Fundraising/Special Event Risks
- Volunteer Risk
- Financial Risk
- Regulatory and Operational Risks
- Staffing Risk
- Reputational Risk
- Information and Data Security Risk

The following steps outline an effective way to conduct an ERA. This does not mean that other processes are not viable or effective, rather this is one way to ensure that all of the goals of an ERA are met. These steps are also presented in a flow chart in Appendix B.

Step 1: Identify areas to assess

There are many areas of risk available to assess, usually referred to as a "risk catalog." There are several places to look for potential risk areas to include, but the following are the most obvious and essential:

1. **Adverse events** within the organization in the past highlight areas of risk *known* to be relevant for the organization. For example, an organization that had a roof collapse due to ice dams over a recent winter, interrupting service in a community-based group home, might identify "severe weather in older buildings" as an area to assess in an upcoming ERA.

   Recognizing that past events can inform the focus of a future ERA, it is recommended that all such events have an "after action analysis" or other debrief to determine:

   a. what caused the event;

b. whether the risk was external or inherent to the organization's operations;
c. whether the outcome had a significant, moderate or minimal effect on the organization;
d. the likelihood of the event occurring again;
e. mitigation efforts prior to the event;
f. effectiveness of how the event was addressed, and whether that response would be appropriate to repeat;
g. whether to increase mitigation efforts immediately going forward.[6]

2. **Organizational Considerations:** after determining risk areas to assess based on past experiences, the organization should consider the organization's mission, strategic plan and programmatic priorities to identify other risk areas relevant to the organization. Appendix D is a sample risk catalog. This is included as a starting point rather than an exhaustive list. This list should not replace an organization's knowledge of its own areas of potential risk – it should be a starting points, from which the ERA team should:
   a. supplement this list with additional, potential risk areas specifically relevant to the organization;
   b. narrow the risk catalog to focus on the most relevant areas for the organization.

   This should be a thoughtful process, focusing on *relevance* rather than priority (priority of relative risks will be assessed in Steps 2 and 3 below). For example, if the organization's services are funded solely by donations and not reimbursement by the federal government, the organization should include any risks related to funding from donors, but does not need to include risks related to the government as a source of funding or reimbursement.

Step 2: Narrow Assessment Topics

Once the organization has identified the areas to be assessed, the next step is to narrow down the topics within those areas to those that are highest priority and most relevant. At this stage it can be helpful to interview key leaders of the organization regarding which topics from the catalog are most relevant for their areas of responsibility.

In larger organizations, where leaders may oversee just one function, it may be appropriate to have those leaders provide input only to the topics most relevant to their function, for example to develop a "top X" list of topics for each

[6] A sample after-action analysis chart is attached as Appendix C.

function. The risk assessment team can then create a list of topics based on both the highest priority topics for *each* function as well as those that are common to *several* functions.

For smaller organizations where a small leadership team oversees the entire organization, it may be most effective to have a leadership meeting to prioritize the topics available for assessment and develop a single list of topics for the organization as a whole.

It is important for the ERA team to take the lead on interpreting the information received and deciding which topics ultimately comprise the assessment topics.

Step 3: Employee and Volunteer Input

Once the risk catalog has been narrowed to those topics most relevant to the organization, the bulk of the ERA rates each potential risk area, usually with input from employees and trusted volunteers, including non-Board and Board volunteers, across functions and levels of the organization. For each of the topics identified, employees should be asked their opinion of four key measures:

a. how often these risk areas come up. The risk assessment terminology for this is "**likelihood**"

b. how serious the outcomes would be, not only financially but to the organization, its reputation and its ability to provide programs and services. The term often used for this is "**impact**."

c. how fast an event in this area would affect the organization. This is the "**velocity**."

d. current efforts the organization takes to minimize risk and the potential effect of the risk in that area, which is referred to as "**current mitigation efforts**."

There are various ways to measure this input – the most common is a "point" scale for each aspect of the risk area. A scale with an odd number of selection points (5-point or 7-point, for example), allows employees to select a "midpoint" option which may be a safe default for many people. For this reason, many risk assessment tools use a 4-point or 6-point scale in order to force everyone to take a position on one side or the other of the mid-line. There is no "correct" way to do this, rather the organization needs to think about its own preferences for rating systems.

Appendix E contains a series of sample questions that an organization might ask about the risks associated with a natural disaster (an "external" risk).

The ERA team can use various ways to obtain employee input. The most common tools are surveys (paper or electronic, possibly using an online survey tool), focus groups and individual interviews. Surveys allow polling of the largest number of employees, and provide the security of anonymity if that would encourage honest feedback. Individual interviews are time-consuming, but provide the opportunity for additional follow-up and discussion. Focus groups provide the opportunity for the ERA team to observe employee discussions and gain tremendous insight into the consistency of opinions. The size and resources of the organization should be considered when deciding which method or combination of methods to use.

If surveys are used, the next step might be to follow up with individual survey participants to ask for additional insight. Individuals can be selected at random, or the ERA team may choose follow up on answers that vary greatly from the more common answers provided by others. If a survey is anonymous, it would be helpful to ask individuals if they are willing to be contacted for more information.

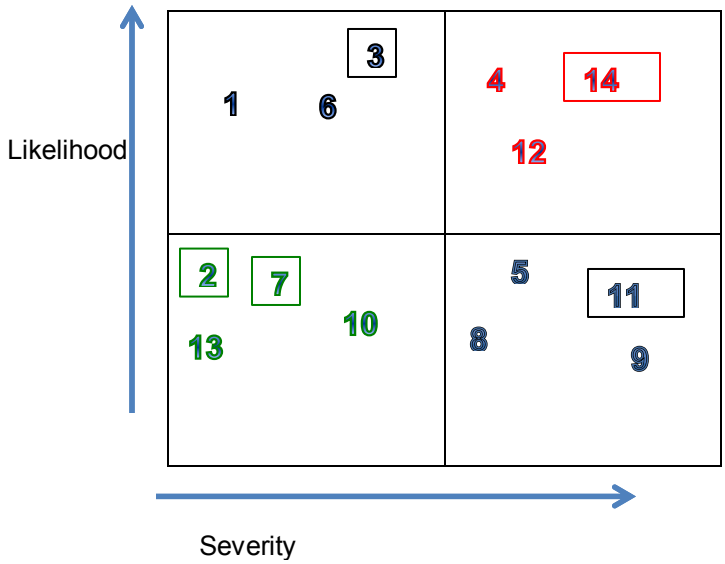
The ERA team can also choose employees at random to interview or join a focus group about the survey results, whether or not they participated in the survey. The preliminary survey results can be an effective discussion generator in interviews or focus groups.

Step 4: Analyze Data

Once the surveys and any interviews or focus groups have concluded, the ERA team reviews the data. Risk Assessment data included for presentation to Leadership and, ultimately, the Board may include:

- critical, medium and low risk areas, both “as is” and adjusted to reflect current mitigation efforts;
- mismatched allocation of resources – for example low impact potential and/or low likelihood but high current mitigation efforts.
- comments from participants from survey or follow up conversations help explain and provide context for the data.

It can be helpful to look at the ERA output in a so-called "heat map." This is a quadrant-based analysis that maps potential risks by likelihood of occurring and severity if they do occur, thus highlighting a quadrant of "hot" areas that are both likely and potentially severe. Then, those areas are mapped against current mitigation efforts. For example:



This sample heat map shows in red those items that are the most likely to occur, and the most potential severity to the organization if they do occur. the items in the "green" quadrant are the least likelihood and the lowest severity. The numbers correspond to the risk items rated by employees.

The speed or "velocity" of impact can be a third factor to include in the heat map analysis. In the above example, the numbers with squares around them were identified in the assessment as having the highest velocity ratings.

The next step would be to review each item again, this time based on the evaluation of current efforts to mitigate these risks to identify:

1. items in "red" above with relatively "low" mitigation efforts;
2. items in "green" above with relatively "high" mitigation efforts.

Through this analysis, an organization can determine whether resources are being allocated appropriately, or if a shift in resources would address the relative risk of each item more effectively. A similar assessment can be done of the items represented in black, but the priority should be to focus on the highest and lowest risks first, where a disproportionate allocation of resources can be most harmful to the organization.

Now that the questions have been asked and answered, it is imperative that the organization develop a plan to address areas of unmitigated serious risk, or overly-mitigated minor risks.

Step 5: Develop and Implement an Action Plan

The Action Plan is a part of the ERA, it is not a separate task. Without it, the results of the ERA may never effect change in the organization, making the process a rhetorical exercise. It is critical that the organization create and implement an action plan based on the ERA outcome. While employees and organization leaders will be responsible for executing the plan, the Board should own oversight of the action plan for implementation of the ERM outcome and recommendations.

Organizations often use a standing or *ad hoc* committee to oversee implementation of the action plan. The most successful risk management strategies incorporate the risk assessment action plan as part of its ongoing strategic initiatives, periodically reviewing the plan and progress towards meeting its goals.

Risk assessments are not a one-time initiative. Risks change as a result of both internal factors (such as expanded or reduced programs or services) as well as external factors (reduced or newly-available funding sources, local or national disasters, etc.). This means that effective risk management incorporates periodic risk assessment. Not every risk assessment has to be enterprise-wide, however. In the time between the bi-annual ERAs, organizations may choose to assess dynamic, discrete areas of the organization more frequently.

An action plan often includes the implementation of an effective compliance program for ongoing risk management. An organizational compliance program is not only part of effective risk management, it is also often required under regulatory requirements.

Under the federal sentencing guidelines, for example, organizations accused of criminal activity can mitigate their fines if they can show they have an effective compliance program designed to prevent employees from violating the law. If the government determines that an organization has most or all of the elements of effective compliance program, it may be fined less than if it did not have an effective compliance program. In other words, if an organization attempted to prevent employees from engaging in unlawful conduct, that organization may be punished less harshly than it would have been otherwise.

Part of having an effective compliance program means that an organization exercises due diligence to prevent and detect criminal conduct, which includes:

a. having relevant policies and procedures to prevent, prohibit and learn about unlawful conduct;

b. high-level oversight of the compliance efforts of the organization, with day-to-day implementation delegated to the appropriate level staff;
c. taking reasonable efforts not to delegate substantial authority to anyone the organization should know has a history of unlawful conduct;
d. ongoing training and communication of the organization's compliance requirements;
e. monitoring and auditing to ensure compliance with the organization's requirements;
f. periodic assessment of the effectiveness of the organization's compliance program;
g. publicized method for individuals to report potential violations of company requirements;
h. consistent incentives for compliant activity and discipline for non-compliant conduct;
i. appropriate responses to inappropriate conduct, including prevention of further inappropriate conduct;

In implementing the above, the guidelines require that organizations *"periodically assess the risk of criminal conduct and . . . take appropriate steps to design, implement, or modify each requirement set forth [above] to reduce the risk of criminal conduct identified through this process."*[7]

Using the outline of an effective compliance program as a guide, the Action Plan can be developed so that each area of the organization is responsible for implementation of tasks related to its own function. The chart included at Appendix F is a sample tool for listing and tracking the various action items by responsible party.

Once the Action Plan tasks have been assigned, there needs to be follow up to ensure that completion of the tasks is on track. This oversight does not need to be the ERA team – in fact, it often makes more sense to assign ownership and oversight of the Action Plan to responsible leadership and Board committee members. For example, the Finance Committee of the Board and the CFO would own and oversee implementation of any tasks assigned to the finance function; the Audit Committee and the head of Internal Audit would own and oversee any tasks assigned to internal audit, and so on. These task owners would report to the ERA team when the tasks are completed, so the implementation can be documented and considered for the next ERA process.

[7] The compliance paradigm discussed above is useful in several contexts. For example, risk mitigation efforts can be structured to address each requirement of an effective compliance program, with appropriate ownership of each element.

CONCLUSION

Enterprise Risk Management, especially periodic Enterprise Risk Assessment, provides structure and cohesion for an organization's risk mitigation efforts. Many of these processes and procedures already exist, and an effective ERA helps each organization's Leadership and Board articulate how they address and mitigate the risks unique to their operational and strategic priorities. This customized approach not only fulfills a requirement of the Federal Performance Monitoring Standards, it is a valuable source of information in responding to an audit or investigation by a government agency.

Appendix A: Privilege

What an organization learns in a risk assessment may reveal legal risks within the organization. As a result, organizations often try to protect the risk assessment data from disclosure to third parties using a type of "privilege." Whether privilege actually attaches to the assessment or resulting data is a legal question that can only be answered on a case-by-case basis. Some general guidelines, however, may be helpful to the context of privilege.

Organizations often try to attach a "privilege" to risk assessment by, for example, having the risk assessment done at the direction of counsel, or saying that it falls under the "self-critical analysis privilege." Practically, however, there are challenges to successfully asserting either of these privileges.

Attorney-Client Privilege

Privilege is a complicated and often-misunderstood concept, even among lawyers. If a communication is subject to the attorney-client privilege that means that the holder of the privilege cannot be compelled by a third party to disclose that communication. In order for a communication to be privileged, it has to be:

1. ***a communication, whether written, electronic or verbal***;
   individuals often opt to communicate verbally with their lawyer so it is not written down, but practically speaking this does not affect the likelihood that the communication will be privileged.
2. ***between a lawyer and a client, with no third parties included***;

   who is "the client" is a question of law that will vary from one organization to another. At a minimum the client will include an organization's senior leader and probably the Board members if the advice is being given to the Board. Mid-level and lower-level managers may be included depending on their actual repsonsibilities and authority within the organization. Non-management employees are generally not "the client," so inclusion of these employees on lawyer-client communication may negate efforts to claim privilege.

3. ***for the purposes of providing or requesting legal advice***.

   efforts to claim privilege often fail here, especially when the lawyer is an in-house attorney. Outside attorneys often provide legal advice, but in-house attorneys often are involved in business decisions as well. Labeling something "attorney-client privileged" or simply copying a lawyer on it does not make it privileged – the role of the parties to the communication and the context of the communication will determine whether that particular communication is privileged. For example, an email from a lawyer to a client containing legal advice may be privileged, but if that client forwards the email to non-management staff or other third

parties as an "FYI" that forwarded email, including the legal advice, is *not* likely to be privileged.

Claiming privilege on a Risk Assessment poses another challenge, which is that it can limit the organization's ability to use that Assessment to its advantage.

Sword and Shield

If an organization is the subject of an audit or investigation by a funder (government or private), the fact that the organization conducted a Risk Assessment may be helpful in that process. In this sense, the Risk Assessment is used a shield during that audit or investigation (i.e. we did the right thing here). While we all believe that we are honest and that the government or funder should just "believe" that we did an appropriate Risk Assessment, they are likely to require production of that Risk Assessment to show that it was done and effective. Thus the "sword" of privilege – "you can't look at this," will most likely need to be waived so that the documents can be used to help the organization.

Strategies for Addressing Privilege

It is possible to conduct a Risk Assessment in a way that the process and outcome will be privileged, or even part of the more complex doctrine of "attorney work product" if the Risk Assessment is conducted by an attorney, but then the organization may be compelled to waive privilege to produce the Risk Assessment in an audit, investigation or legal proceeding. Waiver, however, produces its own risks.

For example, if an organization waives privilege then a court or government agency might argue that the privilege is waived on the *entire* Risk Assessment process, including communications that otherwise fell under the heading of "attorney-client communication."

In addition, if every time an organization waives privilege the underlying information helpful to its situation, that can create an inference when it does *not* waive privilege when the information would be harmful to the organization.

One strategy is to have the Risk Assessment itself *not* privileged, but ensure that a lawyer provides legal advice on the *strategy* of the Risk Assessment process and outcome. An organization's leaders can, for example, request legal advice on customizing the tools in the "How to Conduct A Risk Assessment" section, below, and in the development of an action plan, in an effort to attach privilege to the thought process around what to assess or not.

Because of the nuances of when, how and whether to attach privilege to particular communications, this is something an organization should get legal advice on *before* commencing a Risk Assessment.

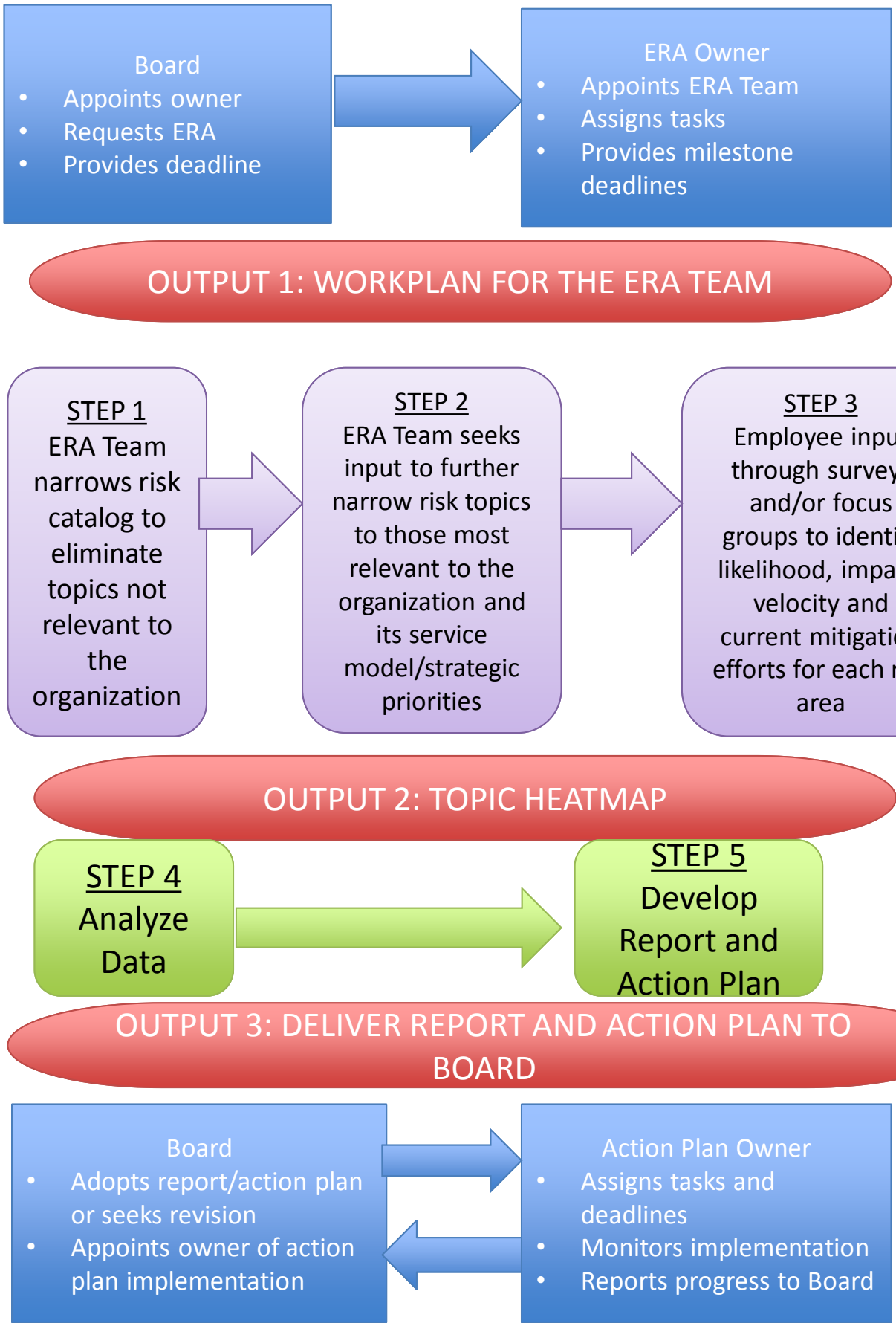
Self-Critical Analysis Privilege

The doctrine of self-critical analysis is less complicated than attorney-client privilege, but is not as widely accepted. Under this theory, it is in the public's best interest for an organization to assess itself to ensure that it is doing the right thing in the best way possible. For example, the public is well served when organizations using public resources or providing a public service looks at its processes, procedures and service delivery in a critical way in order to address errors or attain continuous improvement. In order to encourage organizations to conduct this type of critical self-assessment, courts will sometimes protect that assessment from disclosure to third parties who could use that information against the organization. The theory is intended to encourage the organization and its staff to be honest and open in the assessment process without fear of repercussions based on what is learned.

While on its face this doctrine may seem to apply to Risk Assessment, practically courts ruling on discovery motions in civil and criminal legal proceedings compel disclosure of assessments in most situations. The circumstances that most often lead to protection from disclosure are peer reviews in a clinical context, most often with physicians but sometimes with other health care providers including mental health care.

This means, for example, that a chart review conducted by a peer clinician to assess another clinician's work would likely be protected from disclosure. Courts have recognized that the public will receive better clinical care in the future if peer reviews are candid, so those reviews often are protected from disclosure.

If your organization provides clinical or health care services, your Risk Assessment may have a component that involves a review of those services provided. Thus, your organization may want to ask an attorney if it would be better assess service delivery in a dedicated Risk Assessment rather than as part of an enterprise-wide assessment.


Board
Appoints owner
Requests ERA
Provides deadline
ERA Owner
Appoints ERA Team
Assigns tasks
Provides milestone deadlines
OUTPUT 1: WORKPLAN FOR THE ERA TEAM
STEP 1
ERA Team narrows risk catalog to eliminate topics not relevant to the organization
STEP 2
ERA Team seeks input to further narrow risk topics to those most relevant to the organization and its service model/strategic priorities
STEP 3
Employee input through surveys and/or focus groups to identify likelihood, impact, velocity and current mitigation efforts for each risk area
OUTPUT 2: TOPIC HEATMAP
STEP 4
Analyze Data
STEP 5
Develop Report and Action Plan
OUTPUT 3: DELIVER REPORT AND ACTION PLAN TO BOARD
Board
Adopts report/action plan or seeks revision
Appoints owner of action plan implementation
Action Plan Owner
Assigns tasks and deadlines
Monitors implementation
Reports progress to Board

APPENDIX B

APPENDIX C – SAMPLE AFTER-ACTION ANALYSIS

SAMPLE AFTER-ACTION ANALYSIS FOR CRITICAL EVENTS

Incident/ issue	**Possible to happen again?**	**Can we prevent it?**	**If yes, how?**	**If no, can we mitigate effects?**	**Action plan**
Donor pledge not met	Yes	No	n/a	Yes	Owner: Development Task(s): • Update software to account for “pledges” separate from “donations” • Update reporting to include as “donations” only money actually received (i.e. check cleared, credit card donation received) Due date: 30 days
Federal funding for prevention program not renewed – insufficient enrollment in program	Yes	Yes	More frequent monitoring of enrollment and report under-enrollment to recruiters/intake	Yes	Decrease reliance on individual programs or, where possible, funding sources within individual programs, to minimize impact of lost revenue.

APPENDIX D: RISK CATALOG

GENERAL AREAS OF POTENTIAL RISK:

- Economic
- Environmental
- Geopolitical
- Societal
- Technological
- Programmatic (service delivery)

SAMPLE RISK CATALOG

AVOIDABLE RISKS (Examples)

STRATEGIC	• Failure to meet business objectives • fundraising event inconsistent with mission/goals • inconsistent messaging to public/staff
FINANCIAL – funding	• Uncertain/Loss of funding • denied RFP renewal request • conflict (political, positional) • incomplete, unreliable or improperly reported information • meeting restricted grant obligations
FINANCIAL - invoices	• inaccurate • delayed • fraudulent
FINANCIAL – fundraising	• events fail to meet target
FINANCIAL – investments	• inadequate monitoring • poor understanding of investments • failure to diversify investment portfolio
FINANCIAL – insurance	• underinsurance • no coverage for certain events
FRAUD	• by employees • by Volunteers • by Leadership • by Board
SERVICE DELIVERY	• Abuse of client (i.e. intentional conduct not authorized by organization) ○ by staff ○ by volunteer ○ by authorized “visitor” ○ by non-employee contractor

APPENDIX D: RISK CATALOG

	• Negligence in care of client (i.e. accidents that can result from simply providing services) ○ choking ○ car accident ○ trip/slip and fall ○ services not within standard of appropriate service of that type ○ insufficient/inaccurate documentation ○ spill at program location ▪ hazardous ▪ non-hazardous but dangerous condition ○ food poisoning • Violence ○ by staff ○ by volunteer ○ by authorized "visitor" ○ by non-employee contractor ○ by another client
LEGAL/REGULATORY	• Solicitations • Tax • Recordkeeping/reporting
REPUTATION	• scandal/press regarding an incident • services not delivered as described
PUBLIC/VOLUNTEERS	• Proper vetting and training • trip/slip and fall • spill or other hazard • food poisoning (community event, fundraiser) • Board members' public statements consistent with organization
STAFF/EMPLOYEES/CONTRACTORS	• pay inaccuracies • slip/trip and fall • hazardous exposure • violence (by client, another staff, third party) • allegations of unfair employment practices ○ wage/hour ○ overtime ○ exempt/non-exempt classification ○ leaves of absence ○ reasonable accommodation ○ health insurance ○ timeliness of pay

	○ earned sick time (MA) ○ discrimination/harassment ○ retaliation
LOSS PREVENTION	• theft ○ by staff ○ by volunteer ○ by client ○ by contractor • inaccurate requests for reimbursement ○ fraudulent ○ inadvertent error
DATA PRIVACY	• failure to encrypt where required • improper disclosure (electronic) • improper disclosure (paper)
GOVERNANCE/BOARD MEMBERSHIP	• Conflicts of interest • Proper training/orientation (does the board know what is required of them -- fundraising minimum, time commitment, etc.?)
SUDDEN DEPARTURE (with notice) SUCCESSION PLANNING	• CEO • COO • CFO • CMO/CDO • Volunteer organizer • Board Chair • Audit Committee/Treasurer/Financial Expert

UNAVOIDABLE RISKS (Examples)

FINANCIAL	• Loss of funding ○ financial difficulty of funding source/donor ○ shifted focus of donor/funding source ○ lack of interest in program ○ pledge not met ○ check does not clear bank • Uneven cash flow ○ funding source pay practices (i.e. annual or semi-annual versus monthly) ○ delay in paying invoices for services provided ○ Fundraising event fails to meet target
REPUTATION	• scandal in a similar type of service provider • scandal regarding a strategic partner
SUDDEN DEPARTURE	• CEO

(without notice, for example due to death, appointment to political position, conflict to ongoing assistance)	• COO • CFO • CMO/CDO • Volunteer organizer • Board Chair • Audit Committee/Treasurer/Financial Expert
NATURAL DISASTER	• hurricane • blizzard/ice dams • wind • hail • earthquake • flood • fire • tornado
BOMB THREAT	• at the organization • near an organization program/work site
NATURAL GAS EXPLOSION	• at the organization • near an organization program/work site
HAZARDOUS EXPOSURE	• at the organization • near an organization program/work site
THREATS OF OR ACTUAL VIOLENCE	• terrorism • hostage threat • workplace violence by a third party
LOSS OF DATA OR COMPUTER CAPABILITY (temporary or permanent)	• computer hacking • data loss • server, network or other equipment destroyed or compromised • server, network or other equipment unavailable (*e.g.*, power failure)

APPENDIX E: SAMPLE SURVEY QUESTIONS FOR EMPLOYEE INPUT (STEP 3)

This is an example of survey instructions and questions. Each organization should customize to their specific needs.

NOTE: PLEASE ANSWER THE FIRST TWO QUESTIONS WITHOUT REGARD TO ANY MITIGATION EFFORTS CURRENTLY IN PLACE. YOU WILL HAVE A CHANCE TO RE-RATE THE RISK WITH CONSIDERATION OF ALL MITIGATION EFFORTS. *For example, if the question asked about severity of the risk of a flu pandemic on our employees, clients and patients, you should rate that risk without regard to the availability of a vaccine or any flu treatment. Later you will be asked what measures already exist to mitigate the risk, and then re-rate the risk with consideration of the mitigation efforts.*

(Sample question)
Risk Area: External risks on organization - facilities.

sub-area: natural disasters

What is the likelihood of a natural disaster occurring that would cut off the organization or any of its locations from communication, power, water and transportation?

1 (highly likely)	2	3 (somewhat likely)	4	5 (highly unlikely)

In the event of a natural disaster, such as a hurricane or earthquake, that cuts off communication, water, transportation and power to all of the organization's locations, how would you rate the resulting impact on:

	1 (severe)	2	3 (moderate)	4	5(mild)
Organization's finances					
Ability to provide services					
Employees					
Strategic Partners					
Payors (funding sources)					

In the above situation, how fast would the effects be realized?

	1 (immediately)	2	3 (3-6 months)	4	5 (1 year +)
Financial					
service delivery					
Employee					
Strategic partner					
Payor (funding source)					

APPENDIX E: SAMPLE SURVEY QUESTIONS FOR EMPLOYEE INPUT (STEP 3)

How would you rate current efforts (by the organization or external organizations) to mitigate the impact of this risk?

1 (very little mitigation) 2 3 (risk somewhat minimized) 4 5(effects all but eliminated)

Financial
service delivery
Employee
Strategic partner
Payor (funding source)

1-3 examples of current mitigation efforts would be:
1.
2.
3

[Another way to ask those last two questions would be:

What are 1-3 things the organization or its external partners/funding sources have done to mitigate this risk?

1
2
3

Given this mitigation, how do you rate the current risk as mitigated of a natural disaster?

1 (severe) 2 3 (moderate) 4 5(mild)

Organization's finances
Ability to provide services
Employees
Strategic Partners
Payors (funding sources)]

RISK ASSESSMENT GUIDE FOR NOT-FOR-PROFIT ORGANIZATIONS

APPENDIX F - SAMPLE ACTION PLAN

Each item of the action plan should correspond to an element of an effective compliance program.

Effective Compliance Program Elements*	HYPOTHETICAL SAMPLE:		
	IDENTIFIED RISK: INSUFFICIENT AUDITING OF INVOICES TO FEDERAL GOVERNMENT	**IDENTIFIED RISK:**	**IDENTIFIED RISK:**
	ACTION ITEM: IMPLEMENT RANDOM AUDITS, 3 PER YEAR PER PROGRAM	**ACTION ITEM:**	**ACTION ITEM:**
	DUE DATE: 6 months fully implemented	**DUE DATE:**	**DUE DATE:**
	OWNER: INTERNAL AUDIT AND OPERATIONS	**OWNER:**	**OWNER:**
1. High level oversight, with delegation to individuals for day-to-day compliance responsibilities where appropriate	VP of Internal Audit and Director of each program will oversee audit and report to the Board at quarterly meetings.		
2. Policies and Procedures (company-wide policies as well as function-specific procedures and processes to implement policy requirements)	SOP for audit process to be developed and followed for each audit.		
3. Communication and training (includes formal, tracked training as well as periodic communication via emails and newsletters)	Director of Internal Audit will train auditors on appropriate procedures for auditing billing.		
4. Reasonable care not to delegate substantial authority to individuals with a history of unlawful activity (effective interviewing, background checks, performance reviews)	Ensure that background checks of program and executive leadership were conducted, and monthly checks of SAM debarred list are conducted (Massachusetts requirement).		
5. Ongoing monitoring of compliance with organizational requirements	Board a summary of audit findings every quarter, with plan for remediation of any issues found; Director of Internal Audit to provide to VP of Internal Audit and Board Audit Committee verification of training conducted for audit team members on appropriate procedures for auditing billing.		
6. Ongoing auditing of compliance with organzational requirements	VP of Internal Audit to conduct spot-check of every billing audit for the first year, one audit per year thereafter (or any time there is a new auditor on the team).		
7.Consisitent incentives and discipline for violations	Corrective action to be taken for any deviation from auditing standards; corrective action to be taken for any billing errors, to include re-training on underlying documentation and, if necessary, corrective or disciplinary action for repeat violations.		
8. Reasonable steps to investigate and remediate any inappropriate conduct	Any reported biling errors to be investigated by Compliance/Human Resources, independent of the program staff or any auditors.		
9. Periodic risk assessment	Significant reduction in adverse billing events could lead to improved mitigation "score" in future ERA. Action plan to remain in effect until two years of experience of no adverse billing events. Periodic auditing of invoices to government to remain in effect in perpetuity.		