# Appendix A: Implementation Tools

## OVERVIEW

This appendix provides tools for agencies that are implementing the Commonwealth of Virginia's *Agency Risk Management and Internal Control Standards*. These guidelines and tools represent some suggestions out of many possibilities. **Use of the specific techniques and tools in this appendix is not required for determining whether ARM exists, is complete, or is effective.**

When implementing ARM concepts, agencies should build upon their efforts to develop and maintain a strategic plan, required by *Code of Virginia* § 2.2-5511 and related legislation. Devising a mission, values, goals, objectives, measures, and strategies for a strategic plan builds a foundation for an ARM program. A strategic plan serves as an executive tool for monitoring overall performance, making course corrections, and assessing achievement of goals. Agencies look to the Department of Planning and Budget for guidelines on the basic elements of the Commonwealth's performance leadership system (strategic planning, service area planning, and performance-based budgeting).

Some techniques shown here are illustrative examples, designed to provoke thought as you establish your agency's ARM program. Tools provided will generally be "blank" forms that you may modify for your specific needs. Alternately, you may create your own tools to accomplish the same objectives. ARM policies, processes, skill sets, reports, methodologies, and systems are expected to vary from agency to agency.

Appendix A is organized by these ARM components:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

Since ARM builds on the existing system of internal controls and the strategic plan required by the Code, agencies should already have a foundation for establishing an ARM program. An agency's size, complexity, industry, culture, management style, and other attributes will affect how these *Standards* are most effectively and efficiently implemented. Experience shows that certain commonalities exist. Brief descriptions follow for the common, broad-based actions taken by managements that have successfully implemented ARM.

- **Preparedness** – A core team, with representation from organizational units and key support functions, including strategic planning, is established. This team becomes intimately familiar with the framework's components, concepts, and principles.

- **Executive Sponsorship** – It is important that executive sponsorship be initiated early and solidified as implementation progresses. Executive support, and usually at least initial direct and visible involvement, drives success.

- **Implementation Plan Development** – An implementation plan is developed. The plan should set out key project phases, including defined work streams, milestones, resources, and timing. Responsibilities are identified, and a project management system put in place.

- **Current State Assessment** – This includes an assessment of how ARM components, concepts, and principles currently are being applied across the state agency. This usually involves identifying whatever risk management philosophy has evolved within the organization and determining whether there is uniform core team understanding of the agency's risk appetite.

- **Enterprise Risk Management Vision** – The core team develops a vision that sets out how ARM will be used going forward and how it will be integrated within the organization to achieve its objectives.

- **Capability Development** – The current state assessment and the ARM vision provide insights needed to determine the people, technology, and process capabilities already in place and functioning, as well as new capabilities that need to be developed.

- **Implementation Plan** – The initial plan is updated and enhanced to improve assessment, design, and development. Additional responsibilities are defined, and the project management system refined as needed.

- **Change Management Development and Deployment** – Actions are developed as needed to complement and sustain the ARM vision and desired capabilities – including deployment plans, training sessions, reward reinforcement mechanisms, and monitoring the remainder of the implementation process.

- **Monitoring** – As part of its ongoing management process, management will continually review and strengthen risk management capabilities.

## INTERNAL ENVIRONMENT

**"Internal Environment" is basically the culture and "tone" of an organization and is the basis for all other components of ARM. The internal environment sets the basis for how risk is viewed and addressed by an agency's stakeholders. Environmental factors include risk management philosophy; risk appetite; secretary or board oversight; integrity and ethical values; workforce competence; management assignment of authority and responsibility; and the organization and development of people.**

Management should consider articulating elements of its risk management philosophy in writing. An example of a risk management philosophy follows.

### Exhibit 1: Sample Statement Describing Agency's Risk Management Philosophy

**Exhibit 1: Sample Statement Describing Agency's Risk Management Philosophy**

ARM will provide our organization with the superior capabilities to identify, assess and manage the full spectrum of risks and to enable staff at all levels to better understand and manage risk. This will provide us with:

- Responsible risk assessment and risk response
- Support for Agency Head and the Board
- Improved outcomes
- Strengthened accountability
- Enhanced stewardship

All employees should demonstrate appropriate standards of behavior in development of strategy and pursuit of objectives. This philosophy is supported by following guiding principles. Management and staff shall:

- Consider all forms of risk in decision-making.
- Create and evaluate organizational unit-level and agency-level risk profiles to consider what is best for their individual unit and what is best for the agency as a whole.
- Support executive management's creation of an agency-level "portfolio view" of risk.
- Retain ownership and accountability for risk and risk management at the organizational unit or other point of influence level. Risk management does not defer accountability to others.
- Strive to achieve best practices in ARM.
- Monitor compliance with policies and procedures and the state of ARM.
- Lever existing risk management practices, wherever they exist within the agency.
- Document and report all significant risks and ARM deficiencies.
- Accept that ARM is mandatory, not optional.

To gain insight into how well the risk management philosophy is integrated into an agency's culture, a risk-related culture survey may be conducted. Exhibit 2 (below) shows some of the attributes typically addressed in this type of survey.

## Exhibit 2: Attributes Measured in a Risk-Related Cultural Survey

**Exhibit 2: Attributes Measured in a Risk-Related Cultural Survey**

1. **Leadership and Strategy**
   - Demonstrate ethics and values.
   - Communicate mission and objectives.
2. **People and Communication**
   - Commit to professional and technical competency.
   - Share information and knowledge.
3. **Accountability and Reinforcement**
   - Design organizational structure with risk management in mind.
   - Measure and reward performance.
4. **Risk Management and Infrastructure**
   - Assess and measure risk.
   - Assess security over information and other systems.

Some organizations survey all staff periodically (such as annually) and a representative sample of staff more frequently. The results of such surveys provide indicators of areas of strength and weakness in an organization's culture. The results help the agency identify attributes that need strengthening to ensure an effective internal environment. Exhibit 3 (next page) illustrates how results of a risk-related culture survey question might be presented and interpreted.

## Exhibit 3: Example of a Risk-Related Cultural Survey

**Exhibit 3: Example of a Risk-Related Cultural Survey**

| Question | Attribute | Mean Rating | Assessment | Std. Dev. | Count | SD | D | N | A | SA |
|---|---|---|---|---|---|---|---|---|---|---|
| 1. The leaders of my unit set a positive example for ethical conduct | Leadership and Strategy | 1.42 | Strong | 0.71 | 186 | 1 | 3 | 9 | 77 | 96 |
| 2. I understand the agency's overall mission and strategy | Leadership and Strategy | 1.05 | Good | 0.69 | 186 | 0 | 7 | 18 | 119 | 42 |
| 3. Disciplinary action is taken against those who engage in professional misconduct | Accountability and Reinforcement | 0.21 | Action Needed | 1.20 | 175 | 11 | 55 | 18 | 68 | 23 |
| 4. Turnover of personnel has not significantly affected our ability to achieve objectives | People and Communication | 0.81 | Caution | 0.88 | 145 | 4 | 3 | 39 | 69 | 30 |
| 5. The leaders of my unit are receptive to all communications about risk, including bad news | Risk Management and Infrastructure | 0.99 | Good | 0.85 | 183 | 2 | 13 | 16 | 106 | 46 |

In the preceding example, each question is ranked using a scale of –2 to +2 as follows:

**–2 = Strongly Disagree (SD)**
**–1 = Disagree (D)**
**0 = Neutral (N)**
**+1 = Agree (A)**
**+2 = Strongly Agree (SA)**

The assessment is based on the mean ratings. Additional information is provided by the standard deviation, which is a measure of the respondents' degree of consensus around an issue – the smaller the standard deviation, the greater the respondents' level of agreement on that issue, and the greater the standard deviation, the less agreement.

## Code of Ethics or Code of Conduct

Agencies that actively and continually support a culture of integrity and ethical values communicate these core values through a code of ethics or a code of conduct. Developing and

reinforcing a comprehensive and understandable code is a "best practice" and essential to risk management, linking the agency's mission and vision to its operating policies and procedures. The following table illustrates possible elements of a code of conduct.

## Exhibit 4: Illustrative Structure for a Code of Conduct

| Exhibit 4: Illustrative Structure for a Code of Conduct | |
|---|---|
| **Section** | **Section Outline** |
| 1. Letter from Agency Head | • Presents top management's message on the importance of integrity and ethics to the agency.<br>• Introduces the code of conduct. Gives its purpose and tells how to use it. |
| 2. Goals and Philosophy | • Considers the agency's:<br>○ Organizational culture.<br>○ Programs and types of programs (e.g., regulatory, human services, *et al*).<br>○ Geographic locations.<br>○ Commitment to ethical leadership. |
| 3. Conflicts of Interest | • Addresses conflicts of interest and forms of self-dealing.<br>• Speaks to personnel and those activities, investments, or interests that reflect on the agency's integrity or reputation.<br>• Counsels all employees regarding actual and perceived conflicts of interest, not only those subject to the *State and Local Government Conflict of Interests Act* (*Code of Virginia* § 2.2-3100 *et seq.*). |
| 4. Gifts and Gratuities | • Deals with giving or receiving of gifts and gratuities, setting forth the agency's policy, typically going beyond legal requirements.<br>• Sets standards and provides guidance regarding gifts and entertainment and their proper reporting. |
| 5. Transparency | • Includes provisions dealing with the agency's commitment to complete and understandable social, environmental, and economic reporting. |
| 6. Agency Resources | • Includes provisions dealing with agency resources, including intellectual property and proprietary information – to whom these belong to and how they are safeguarded. |
| 7. Social Responsibility | • Includes the agency's role as a citizen, including its commitment to human rights, environmental sustainability, community involvement, and environmental and economic issues. |
| 8. Additional Conduct-Related Topics | • Includes provisions regarding adherence to policies established within specific areas of agency activity, for example:<br>○ Employment issues such as fair labor practices and antidiscrimination.<br>○ Governmental dealings such as contracting, lobbying and political activity.<br>○ Antitrust and other competitive practices.<br>○ Good faith and fair dealing with citizens, clients, suppliers, and others.<br>○ Confidentiality and security of information.<br>○ Safety and quality in our programs' services. |

## OBJECTIVE SETTING

**"Objective Setting" is the process that identifies objectives at a strategic level, then sets supporting operational, reporting, and compliance objectives. Objectives at both levels must exist before management can effectively identify events, assess risk, and establish risk responses. ARM ensures that management has a process in place to set objectives and that the chosen objectives support and align with the agency's mission and are consistent with its risk appetite.**

Agency level objectives are linked to and integrated with more specific objectives that cascade throughout the organization to sub-objectives established for various activities. Exhibit 5 is a teaching hospital's mission with strategic objectives, strategies, and related objectives.

### Exhibit 5: Linking Mission, Vision, Strategic Objectives, and Operational Objectives

| Exhibit 5: Linking Mission, Vision, Strategic Objectives, and Operational Objectives | |
|---|---|
| **The mission, vision, strategic objectives, and operational objectives to which this tool refers are those developed under DPB guidelines (www.dpb.virginia.gov/sp/userguide2005.pdf).** | |
| **Mission** | To maintain world-class research and medical instruction while providing our metropolitan community with high quality, accessible, and affordable patient care |
| **Strategic Objectives** | • Provide superior, compassionate, and innovative patient care to improve the health of all members of the communities we serve<br>• Be recognized on the East Coast as a premier medical facility, especially for cardiac and transplant services |
| **Strategies** | • Develop programs to attract top teaching physicians and students<br>• Enhance our infrastructure systems to provide effective management and cost control<br>• Achieve a leading track record of compliance with all healthcare and other applicable laws and regulations |
| **Related Objectives** | |
| **Operations** | • Identify specific areas of future medical staff needs and develop a marketing program to attract top research and teaching physicians<br>• Implement new systems to track all aspects of patient care<br>• Identify any deficiencies in our patient care and educate our staff in ways to eliminate those deficiencies |
| **Reporting** | • Upgrade our systems to provide management reports on key performance measures, with exception and trend line analysis, within four working days of month-end<br>• Ensure all departments report, accurately and on a timely basis, compliance performance and issues for management review<br>• Establish uniform reporting system and account structures for assembly of accurate and complete information required for external reporting |
| **Compliance** | • Establish central compliance office with charter, leadership, and staffing to support individual units<br>• Ensure line personnel recognize their primary compliance responsibilities, building those into human resource objectives and performance assessments<br>• Review and upgrade hospital-wide protocols for patient care, medical procedures, drug storage and dispensing, staff assignments, and scheduling<br>• Review privacy policies and practices, and then benchmark against federal requirements and best practices |

Risk appetite, established by management (with board or secretarial oversight, when applicable) is a guidepost in strategy setting. An agency may consider risk appetite qualitatively or quantitatively. Exhibit 6 (below) provides illustrative questions management might ask when considering its risk appetite.

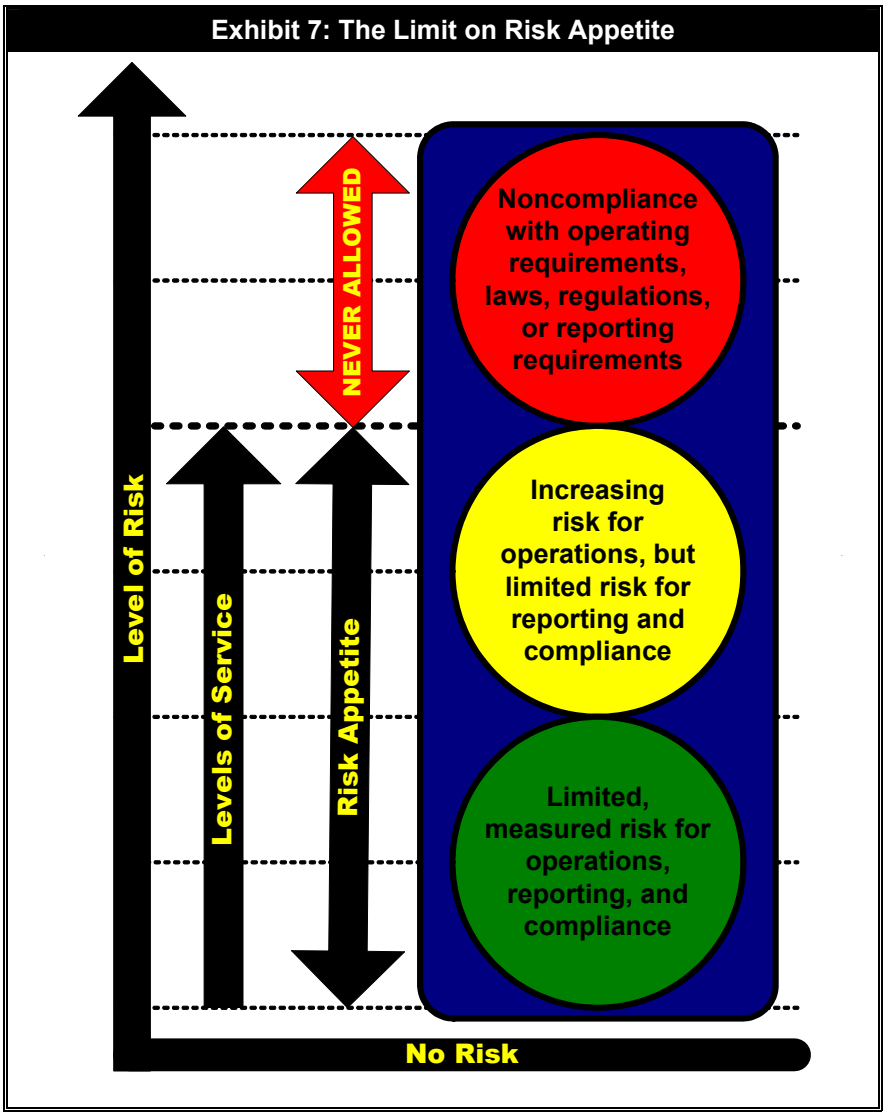
## Exhibit 6: Considering Risk Appetite

**Exhibit 6: Considering Risk Appetite**

1. What risks is the agency willing to accept? For example, is the agency willing to accept minor losses of physical inventory from pilferage (due to the high cost of increased control) but not willing to accept large losses of physical inventory from spoilage, obsolescence, or natural disasters?
2. Is the agency comfortable with amount of risk accepted, or to be accepted, by each of its units?
3. Has the agency taken full advantage of opportunities to avoid, reduce, and share risk?
4. What specific risks will the agency not accept, such as risks that could result in non-compliance with information privacy, prompt payment, and other laws?
5. Is the agency more comfortable with qualitative or quantitative measures of risk?
6. What risks is the agency willing to accept regarding possible reduction in funding and personnel?
7. What risks is the agency willing to accept regarding the impact of new legislation or regulations?
8. What risks is the agency willing to accept that may result from changes in the commercial, political, or economic climate?
9. What risks is the agency willing to accept that may result from problems encountered by major suppliers and contractors?
10. What risks is the agency willing to accept that may result from disruption of information systems processing?

The concept of risk appetite does not allow an executive to take higher levels of risk than are prudent for a steward of the public's resources. Financial reporting and compliance objectives must not be threatened in pursuit of program goals. An agency head's risk appetite must be confined to one that fits the following model.

## Exhibit 7: The Limit on Risk Appetite



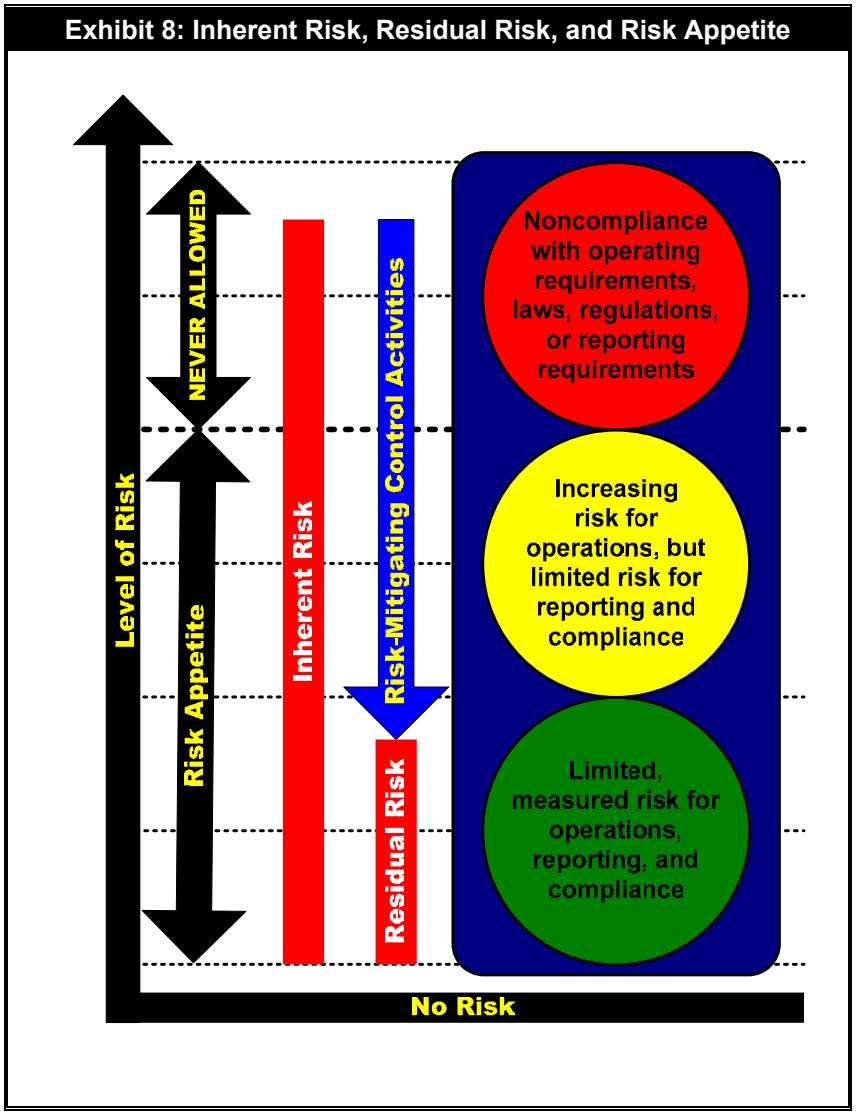

**LIMITS ON ACCEPTING RISK**

- **Agencies cannot jeopardize meeting their compliance or financial reporting objectives, regardless of individual willingness to accept risk.**
- **A higher or lower risk appetite may be adopted, so long as both compliance and financial reporting objectives are met.**
- **Risk appetite may be raised to increase service or quality, as long as both compliance and financial reporting objectives are met.**
- **No matter how low your risk appetite, "no risk" is not possible due to cost limitations.**

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. For example, an agency has an objective of on-time delivery at 98%, with acceptable variation in the range to 96%. Alternately, an institution wants response to all customer complaints within 24 hours, but accepts that up to 25% of complaints may receive a response within 24-36 hours.

If inherent risk is too high, managers may be able to identify a cost-effective strategy or combination of strategies to avoid, reduce, or share the inherent risk. If these strategies put an activity's residual risk within the agency's risk appetite, the activity may be undertaken.

## Exhibit 8: Inherent Risk, Residual Risk, and Risk Appetite




This exhibit illustrates the effect of cost-effective control activities on risk; unmitigated inherent risk could prohibit the activity, but residual risk falls well within the risk appetite due to controls.

## EVENT IDENTIFICATION

**"Event Identification" is the process of identifying potential internal and external events that will, if they occur, affect achievement of agency objectives. Management must identify these events and determine whether they represent risks or opportunities. Risks will have a negative impact and require management's assessment and response. Opportunities are channeled back to management's strategy or objective-setting processes.**

In some circumstances, identifying events relate straightforwardly to a specific objective. Exhibit 9 exemplifies of this relationship.

### Exhibit 9: Identifying Events Linked to Mission and Objectives

| Exhibit 9: Identifying Events Linked to Mission and Objectives | | |
|---|---|---|
| Strategic Planning | 1. Mission | To provide high quality, accessible, and affordable patient care to all patients using our facilities |
| | 2. Strategic Objective | To provide quality care to all patients and at a minimum, satisfy the regulations regarding nurse to patient ratios in all areas of the hospital. |
| | 3. Related Operational Objective | Hire 40 new qualified nurses |
| | 4. Operational Objective's Unit of Measure | Number of new qualified nurses hired |
| Risk Management | 5. Consider Risk Appetite and Determine Risk Tolerance | 37 – 43 qualified nurses hired |
| | 6. Identify Potential Events, Risks, and Related Impacts | • Unexpected slowdown in job market causing more offers being accepted than planned, resulting in excess staff<br>• Unexpected heating up of job market causing fewer offers being accepted, resulting in too few staff<br>• Inadequate needs, specifications, or descriptions, which could result in hiring unqualified persons |

The most important task in risk assessment may be event identification. In this context, an "event" usually is thought of as "something that could go wrong." However, be alert for "what could go better than expected," as well. The creative process of event identification is where risk management begins to expand on information captured in strategic plans. An agency may use various techniques for event identification; more information and related exhibits follow for these techniques:

- **Event Inventories** (Exhibit 10)
- **Facilitated Workshops** (Exhibit 11)
- **Interviews** (Exhibit 12)
- **Questionnaires and Surveys** (Exhibit 13)
- **Process Flow Analysis** (Exhibit 14)
- **Leading Event Indicators** (Exhibits 15 and 16)
- **Escalation Triggers** (Exhibits 17 and 18)
- **Loss Event Data Tracking** (discussion on page 44)

## Exhibit 10: Event Inventories

Event inventories are listings of potential events that may be common to an agency or program. The list is developed by personnel within the agency, not only from past experience but also from information about the future gleaned from the *Roadmap for Virginia's Future*, bills expected to be submitted to the General Assembly, news media, research publications, political and professional organizations, and similar sources. Exhibit 8 illustrates the use of an externally produced inventory of events potentially affecting a software development project.

| Exhibit 10: Illustration of an Event Inventory |
| --- |
| Before undertaking a software development project, an agency reviews an inventory of generic risks inherent in software development projects that appeared in an information technology journal article. The inventory provides a useful way to draw on the accumulated risk knowledge of others experienced in this subject area. Recognizing that the inventory includes risks from organizations with different characteristics, management considers the effect of these risks on its own unique circumstances. |

A senior management workshop could identify events that could affect achievement of agency strategic objectives, and link those potential events to specific objectives as shown in Exhibit 10 on page 37. Exhibit 11 (next page) illustrates one way to organize a facilitated workshop for the purpose of event identification.

## Exhibit 11: Plan for a Facilitated Events Identification Workshop

**Exhibit 11: Plan for a Facilitated Events Identification Workshop**

**Before The Workshop**

- Identify an experienced facilitator to lead the session, manage group dynamics, and plan how to capture generated ideas in usable form
- Establish and agree on ground rules when the workshop opens
- Recognize differences in participant styles and personality types, considering how to optimize their contribution
- Identify which objectives, category of objectives, and categories of events to focus on
- Invite an appropriate number of workshop participants – usually 15 or fewer
- Set realistic expectations regarding what the workshop is intended to achieve

**Workshop Agenda**

1. **Introduction**
   - Explain background of workshop and why each participant has been invited
   - Explain ground rules
2. **Explain workshop process**
   - Events are to be considered against agency objectives
   - For each objective, the facilitator will prompt discussion on events emanating from the following factors, and their related effects:

| External | Internal |
|---|---|
| Economic | Infrastructure |
| Natural environment | Personnel |
| Political | Process |
| Social | Technology |
| Technological | |

   - Describe how and when voting tools and verbal inputs will be used
   - Explain how ideas, conclusions will be documented
3. **Explore Objectives and Identify Events**
   - Identify each objective, its unit of measure, and the related established targets
   - Gain consensus of risk tolerance, the degree of acceptable variation around the unit of measure
   - Discuss internal and external factors that drive potential events relative to the objective
   - Determine which events represent risks to achieving the objective, and which events represent opportunities
   - Consider how multiple risks affecting this objective relate to one another
4. **Next steps and close**
   - Distribute the workshop output to all participants within 48 hours, with action plan for next steps

In contrast to workshops involving many people, interviews can be conducted to plumb candid personal views on actual past events and potential future events. Exhibit 12 illustrates an interview agenda with a focus on organizational unit objectives.

## Exhibit 12: Interview Agenda

**Exhibit 12: Interview Agenda**

**Interview Agenda**

1. Introduction
2. Provide background on the project and interview process
3. Confirm the person's position, background, and current responsibilities
4. Confirm they received and read any background material provided in advance

**Strategies and Objectives**

1. Identify the key objectives within the interviewee's organizational unit or division
2. Determine how the objectives align with and support the agency's strategies and objectives
3. Identify the unit of measure for each objective and the related established targets
4. Determine the established risk tolerances
5. Discuss factors related to potential events relative to the objective
6. Identify potential events that create risks for objectives, and identify potential events that pose opportunities
7. Consider how the interviewee prioritizes these events, considering likelihood and impact
8. Identify events that have occurred in the past 12 months that impacted the agency that were not identified by management and staff
9. Consider whether risk identification mechanisms need to be enhanced

Questionnaires help participants to focus on internal and external factors that have given rise to or may give rise to events. They can be directed to individuals an agency, customers, suppliers, or other external parties. Exhibit 13 (next page) illustrates this technique.

## Exhibit 13: Using Targeted Questionnaires

**Exhibit 13: Using Targeted Questionnaires**

**Targeted Questionnaire**

An agency requires purchasing department buyers to complete a questionnaire before accepting a new vendor. The questionnaire requires the buyer to consider a range of questions exploring the potential vendor's:

- Quality processes
- Risk management processes
- Insurance coverage
- Terms and conditions

In considering the questions, the buyer identified these potential events to which the agency would be exposed if it did business with the vendor:

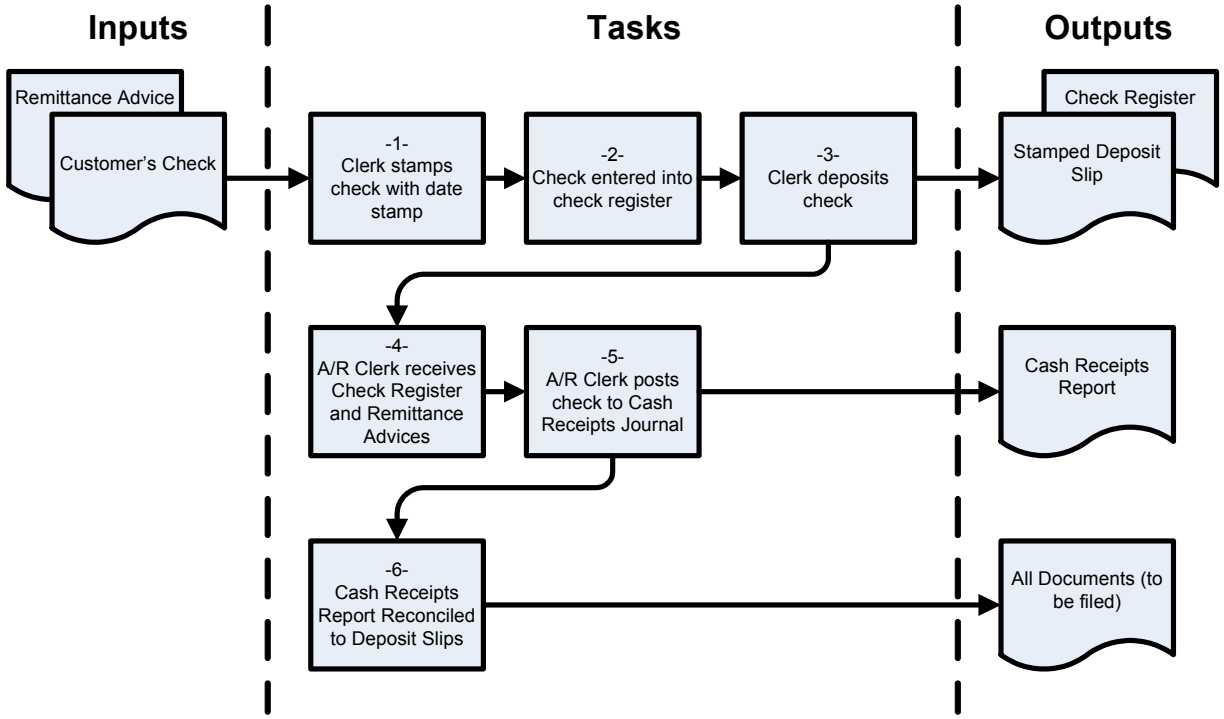
- The vendor's history of inconsistent delivery presents a risk of supply chain disruption.
- The vendor is not certified to an appropriate quality standard. A risk exists that its products might not meet agency quality specifications, causing service problems and reputation damage.
- The vendor has inadequate insurance coverage for product defects. A risk exists that the agency would not be able to recover associated losses.
- The vendor's terms require a two-year commitment from the agency, with an associated risk of changing needs and related economic loss.

Surveys are another event identification technique. For example, an agency may survey its clients to determine their preferences and satisfaction levels with the service provided by the agency. A survey may identify a shift in preferences or satisfaction levels with service. With this information, management can assess the extent to which the shift in preferences and decline in customer satisfaction levels, calls for modification of strategy and related objectives.

## Exhibit 14: Process Flow Analysis

Process flow analysis involves diagramming a process to better understand interrelationships among process inputs, tasks, outputs, and responsibilities. Once diagrammed, events can be identified and considered against process objectives. Exhibit 14 shows a cash receipts process mapped to identify risks related to the objective of depositing and recording all cash receipts on a timely and accurate basis.

**Exhibit 14: Process Flow Analysis**




| Tasks | Possible Events |
|---|---|
| 1. Clerk stamps check with date stamp | • Clerk fails to stamp check |
| 2. Check entered into check register | • Clerk fails to record check details<br>• Clerk records incorrect check details<br>• Clerk misappropriates check |
| 3. Check deposited by Clerk | • Check lost while in route to bank<br>• Check deposited to incorrect bank account<br>• Incorrect amount recorded by bank<br>• Stamped deposit slip lost |
| 4. Remittance slips and check register sent to accounts receivable clerk | • Remittance slips or check register misplaced or lost |
| 5. Accounts receivable clerk posts checks to Accounts Receivable ledger | • Checks applied to incorrect accounts<br>• Incorrect amount recorded against customer account<br>• Accounts receivable clerk does not post checks |
| 6. Posting report matched to deposit slip | • Details do not match |

## Leading Risk Indicators and Escalation Triggers

Leading risk indicators (or "leading event indicators") are qualitative or quantitative measures that provide insight into potential events. To be useful, management must have leading risk indicators on a dependable and timely basis (perhaps daily, weekly, monthly, or in real time).

Escalation triggers typically focus on day-to-day operations and are reported on an exception basis, when a pre-established threshold is passed. To be effective, escalation triggers must come to managers' attention with sufficient lead to take action.

## Exhibit 15: Examples of Leading Risk Indicators and Escalation Triggers

**Exhibit 15: Examples of Leading Risk Indicators and Escalation Triggers**

| Organizational Unit's Objective | Measure | Target and Tolerance | Potential Event | Leading Indicator | Escalation Trigger for Organizational Unit |
|---|---|---|---|---|---|
| Create and maintain strong security against external intrusions on systems | Number of successful intrusions | **Target:** 0 per month<br>**Tolerance:** 0 per month | Unauthorized individuals access the agency's systems via Internet ports | Detected vulnerabilities in the agency's operating systems published by the vendor or third party; number of unauthorized attempts | New critical vulnerabilities identified by third parties |
| Comply with standards governing the movements of hazardous material | Volume of spills of hazardous materials | **Target:** <100 gallons per year<br>**Tolerance:** 0 to 125 gallons | Corrosion on barrels causes material to leak from trucks during transport | Age of barrels used to transport hazardous material | Barrels in use for more than 85% of their estimated useful life |
| Maintain stable high-quality workforce | Turnover of staff rated as high performers | **Target:** Turnover of high performers <10%<br>**Tolerance:** 2% – 12% | High performers resign | Staff morale of high performers | High performers responding as "very" or "somewhat" dissatisfied in annual employee survey |

## Loss Event Data Tracking

Loss event databases contain information on actual events meeting specified criteria. This can be a useful source of information for identifying trends and root causes. It may be more effective for management to assess and treat a root cause than to address individual events. For example, an agency operating a large automobile fleet maintains a database of accident claims and through analysis finds that a disproportionate percentage of accidents (in number and cost) are linked to drivers in particular units, locations, and age brackets. This analysis equips managers to identify root causes and take action. Tracking may rely on internally or externally generated data.

## Exhibit 16: Leading Event Indicator Mechanisms

The event identification techniques discussed thus far are typically applied on an ad hoc basis. In addition to ad hoc activities, routine activities also can identify potential events. The discussion of Exhibit 8 (page 38) mentions external sources of information from which events can be gleaned. Exhibit 14 (below) lists some external information sources that an agency can monitor and from which potential events may be identified.

**Exhibit 16: Leading Event Indicator Mechanisms**

| | External Factors | | | | | Internal Factors | | | |
|---|---|---|---|---|---|---|---|---|---|
| Mechanism = Input From: | Economic | Natural Environment | Political | Social | Technological | Infrastructure | Personnel | Process | Technology |
| Virginia Department of Emergency Management (http://165.176.249.147/library/eopvol6/2002/part_three.pdf) | | ♦ | | | | ♦ | ♦ | | |
| Industry or technical conferences | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ |
| Political lobbyists | | | ♦ | | | | | | |
| Internal risk management meetings | | | | | | ♦ | ♦ | ♦ | ♦ |
| Benchmarking reports | ♦ | | | | ♦ | ♦ | ♦ | ♦ | ♦ |
| Key external indices | ♦ | ♦ | ♦ | ♦ | ♦ | | | | |
| Key internal indices | | | | | | ♦ | ♦ | ♦ | ♦ |
| Risk and performance measures and scorecards | | | | | | ♦ | ♦ | ♦ | ♦ |
| New legal decisions | ♦ | | ♦ | ♦ | | | | | |
| Media reports | ♦ | ♦ | ♦ | ♦ | ♦ | | | | |
| Monthly management reports | | | | | | ♦ | ♦ | ♦ | ♦ |
| Analyst reports | ♦ | | ♦ | ♦ | | | | | |
| Electronic bulletin boards and notification services | ♦ | ♦ | ♦ | ♦ | ♦ | | | | |
| Industry, trade, and professional journals | ♦ | ♦ | ♦ | ♦ | ♦ | | | | |
| Profiling calls to customer service | ♦ | | | | ♦ | | | ♦ | |
| Real-time feeds of financial market activity | ♦ | | | | | | | | |

## RISK ASSESSMENT

**"Risk Assessment" is the process of analyzing potential events, considering likelihood and impact, as a basis for determining what impact they may have on the achievement of objectives. Risks are assessed on an inherent and a residual basis.**

Inherent risk is risk in the absence of any management action to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management's response to the risk. Risk assessment is applied first to inherent risks. Once risk responses – avoiding, accepting, reducing, or sharing risk – have been developed, management then considers residual risk. It is important for management to adequately document the risk assessment process. The following example of an inherent risk assessment links risks to objectives.

### Exhibit 17: Example of Inherent Risk Assessment

| Exhibit 17: Example of Inherent Risk Assessment | | |
|---|---|---|
| Operations objective | Hire 40 new qualified nurses across all hospital departments to provide quality care to all inpatients and at a minimum, satisfy the regulations regarding nurse to patient ratios in all areas of the hospital | |
| Objective unit of measure | Number of new qualified nurses hired | |
| Tolerance | 37– 43 qualified nurses hired | |
| Risks | **The Inherent Risk Identified** | |
| | **Likelihood** | **Impact** |
| Insufficient number of qualified candidates available | 20% | 10% reduction in hiring – 4 unfilled positions |
| Initial candidate screening filters too stringent | 30% | 5% reduction in hiring due to poor candidate screenings – 2 unfilled positions |

Estimates of risk likelihood and impact often are determined using data from past observable events (see Loss Event Data Tracking, page 44) that provide objective decision making, rather than relying entirely on subjective estimates.

An agency's risk assessment methodology should use a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification, insufficient credible data is not available, or obtaining

and analyzing data is not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques.

An agency does not need to use common assessment techniques across organizational units. For example, it may be appropriate to use self-assessment questionnaires in one unit and workshops in another. Although different methods are used, they provide sufficient consistency to facilitate assessment of risks across the agency.

Methodologies for assessing risk should be applied to the same time frame as the related strategy and objectives. If strategy and objectives focus on short to mid-term time horizons, management should assess risks associated with those time frames. If a strategy and objectives extend to the long term, management should not ignore risks that might appear further into the future.

Exhibit 18 portrays a qualitative assessment.

## Exhibit 18: Ranking the Next Quarter's Computer Operations Risks by Likelihood

| Exhibit 18: Ranking the Next Quarter's Computer Operations Risks by Likelihood | | | |
|---|---|---|---|
| **Level** | **Assessment** | **Likelihood** | **Risk** |
| 1 | Rare | Very low | Technology systems shut down for prolonged periods by terrorist or other intentional action |
| 2 | Unlikely | Low | A natural disaster or third party (e.g., utility) event requires invoking the operational continuity plan |
| 3 | Possible | Moderate | Hackers penetrate our computer security |
| 4 | Likely | High | Internal staff use agency resources to access inappropriate information from the Internet |
| 5 | Almost certain | Very high | Internal staff use agency resources for personal messaging |

Exhibit 19 (next page) serves as an example for assessing risks related to implement new information systems, using categorization and risk rankings of low, moderate, and high.

## Exhibit 19: Risk Assessment for New Information Systems

**Exhibit 19: Risk Assessment for New Information System Implementation**

**Objective** ..... Implement a new information system to oversee federal and state legal compliance

**Risk**..... The project takes longer to complete than expected

| Category | Question | Response | Likelihood |
|---|---|---|---|
| Personnel | What is the experience of project team members? | At least one staff member has successfully implemented such system before | Low |
| | | At least one staff member has implemented such system before, but with mixed results | Medium |
| | | No team member has done this before, or has with negative results | High |
| Management process | How stable is the management team? | Stable management team with average tenure >2 years | Low |
| | | Changing management team with average tenure between 1 and 2 years | Medium |
| | | New management team with average tenure <1 year | High |
| Vendor | How well known is the technology vendor? | Expansion of current services with alliance partner | Low |
| | | New service with existing vendor | Medium |
| | | New vendor | High |
| Implementation process | How well established is the implementation process? | Proven methodology | Low |
| | | Existing methodology in place, but used with mixed results | Medium |
| | | New methodology | High |
| Regulatory | How well are regulatory requirements known? | Regulatory requirements are well established | Low |
| | | Regulatory requirements are unclear or subject to periodic amendment | Medium |
| | | Regulatory requirements are unknown or frequently subject to substantial change | High |
| Continuity plan | How well tested is the continuity plan for this project? | Successfully tested continuity plan for the new application | Low |
| | | Tested continuity plan for the new application, with significant needed fixes identified | Medium |
| | | No continuity plan in place for the new application | High |

## Formal Statistical Analysis Techniques

Professional statisticians typically perform quantitative assessment techniques. These methods depend highly on the existence and quality of supporting historic data, assumptions, and statistical applications software. These methods are most relevant for past events for which appropriate data has been captured, providing a known history to support reliable mathematical forecasts. Examples of quantitative risk assessment techniques include:

- Benchmarking techniques
  - Internal
  - Competitive or industry
  - Best-in-class
- Probabilistic models (associate a range of events and resulting impact with the likelihood of those events, based on certain assumptions)
  - Value at risk
  - Cash flow at risk
  - Earnings at risk
  - Credit and operational loss distribution
- Non-probabilistic models (use subjective assumptions to estimate event impact without quantifying an associated likelihood)
  - Sensitivity measures
  - Stress tests
  - Scenario analyses

These statistical techniques apply primarily to for-profit organizations, often in such functions as cash and investment management and product pricing. Although these techniques may not be applicable in most agencies, those with statistical analysis capabilities may find opportunities to employ these or other techniques, particularly for enterprise and internal service fund programs. Agencies that have developed alternate models for formal statistical analysis to support risk management and internal control are encouraged to continue using and to share those techniques with other agencies.

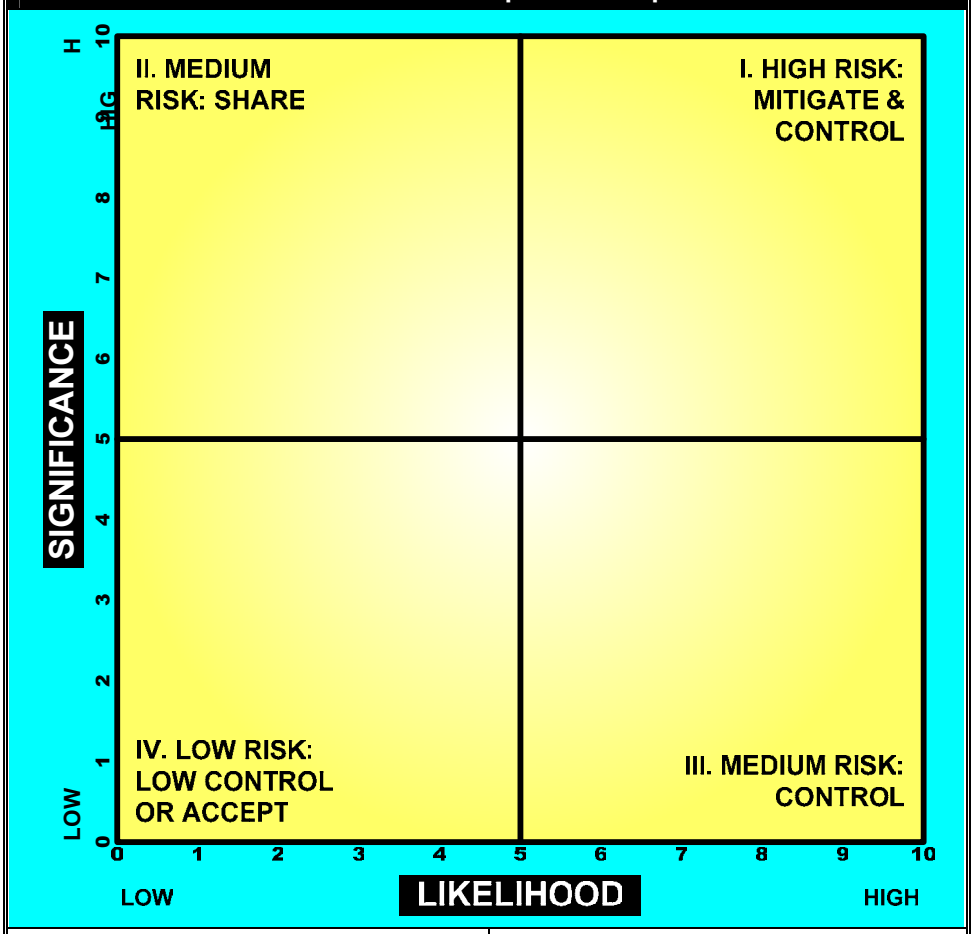
## Portraying Qualitative Risk Assessments

Risk assessments can be portrayed in different ways. Portraying risks in a clear and concise manner is especially important with qualitative assessment because some risks cannot be summarized in numeric rankings. Such techniques include risk maps and non-numerical representations.

A risk map prioritizes each risk according to significance and likelihood and maps the risks into four quadrants. Sample risk maps appear as Exhibits 20 and 21. Risk maps have the effect of visually grouping events into one of four groups, for which similar levels of overall risk exist and for which similar combinations of risk responses may be appropriate. ARM authors vary in how they describe responses to events in each of the four quadrants; for this model, general descriptions of risk response strategies for each quadrant appear at the bottom of Exhibit 20.

## Exhibit 20: Sample Risk Map

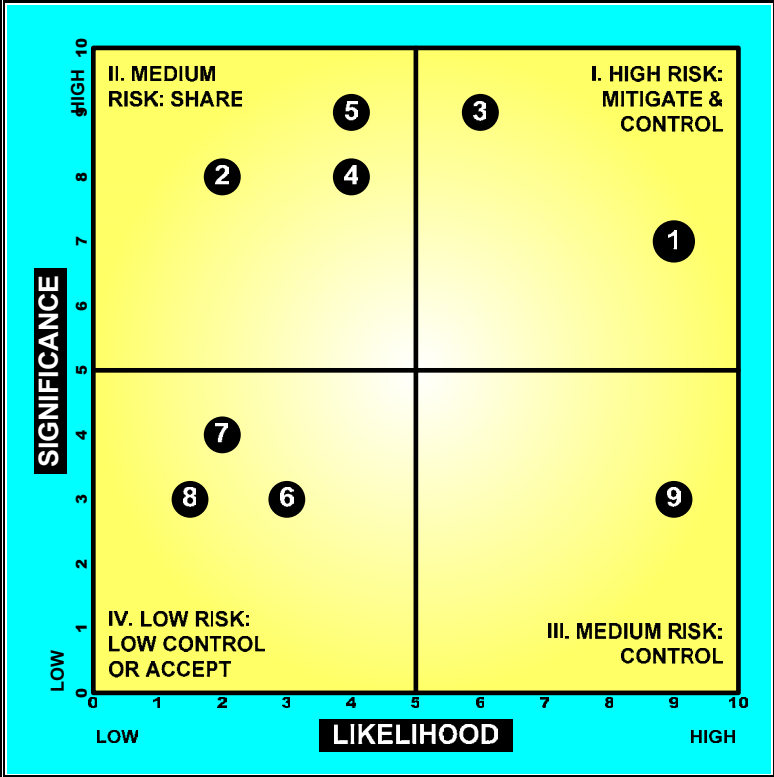
**Exhibit 20: Sample Risk Map**




| **Quadrant II – Share Risks** | **Quadrant I - Mitigate and Control Risks** |
|---|---|
| Some events are unlikely, but could occur for an agency or location with major or catastrophic consequences. Such events include vehicular collisions, on-the-job injuries, fire damage to state facilities, and major thefts. A common means of sharing such unlikely but high-impact events is insurance. | Risks are both significant in consequence and likely to occur. Inherent risk must be reduced with preventative controls, with subsequent internal control to ensure that preventative controls remain adequate and work properly. Risks in this quadrant include escapes from correctional institutions, livestock disease outbreaks that threaten food supplies, and hurricanes. |
| **Quadrants IV – Low-Control or Accept Risks** | **Quadrant III – Common, Low-Impact Risks** |
| Risks in this quadrant are both unlikely to occur and not significant. They require minimal monitoring and control unless subsequent risk assessments show a substantial change, prompting a move to another risk category. (Note: acceptance applies only to operational risk; reporting and compliance risks may not be accepted.) | Events are less significant but likely to occur if adequate controls are not established and operating effectively. Risks include theft or embezzlement of cash and the theft of equipment such as autos, personal computers, and digital cameras. These risks should be monitored to ensure that control activities mitigate such risks. |

## Exhibit 21: Sample Risk Map for a Telephone Hotline

**Exhibit 21: Sample Risk Map for a Telephone Hotline**




An employee survey asked each person to quantify the significance and likelihood that any of the following nine events would occur. The events and average scores appear below, while corresponding event numbers appear on the risk map above.

| Event | Significance | Likelihood |
|---|---|---|
| 1. Callers have long waits | 7 | 9 |
| 2. Information capture errors | 8 | 2 |
| 3. Insufficient staff to handle calls | 9 | 6 |
| 4. Loss of phone services | 8 | 4 |
| 5. Loss or corruption of database | 9 | 4 |
| 6. Lost records of calls received | 3 | 3 |
| 7. Low employee morale | 4 | 2 |
| 8. Malicious (fraudulent) calls | 3 | 1.5 |
| 9. Repeat calls for same problem | 3 | 9 |

## Exhibit 22: Non-Quantitative Risk Assessment for Accounts Payable

The preceding example assumes that significance and likelihood can be quantified, either based on actual measurements or numeric estimates. However, actual data may not be available for measurement and numeric estimates may be deemed unreliable; in those cases, a completely subjective "measure" may be used.

Exhibit 18 (below) and Exhibit 19 (page 54) illustrate risk assessments for the accounts payable and fixed assets functions that rely on non-numeric "measures" of risk. These non-probabilistic tools offer subjective estimates of event impact (low, medium, and medium with verbal qualifications) without an associated percentage likelihood.

**Exhibit 22: Non-Quantitative Risk Assessment for Accounts Payable**

| Risk | Control | Control In Place | Risk Assessment |
|---|---|---|---|
| Payment made to incorrect vendor | Department authorizes payment by matching vendor invoice and receiving report to purchasing system. Accounts payable matches invoice, purchase order, and receiving report to purchasing system. | Yes. | Low |
| Invoices paid after due date | An accounts payable supervisor periodically reviews unpaid invoices appearing in the purchasing system and in the general ledger. | Yes. However, review is manually (visually) performed by reviewing the "Document Authorization Mailbox" screens. This process is tedious, time-consuming, and subject to error. No system exception reports are available to specifically identify untimely processing. | Low |
| Incorrect amount paid to vendor | Purchasing system requires matching of prices and quantities from the purchase order to the invoice. Tolerance level is $25 or less. Any difference requires department or purchasing office's approval. Also, see first risk assessment control. | Yes. | Low |

| Exhibit 22: Non-Quantitative Risk Assessment for Accounts Payable | | | |
|---|---|---|---|
| **Risk** | **Control** | **Control In Place** | **Risk Assessment** |
| Duplicate payment made to vendor | Supporting documents are cancelled with perforator by accounts payable. In addition, purchasing system prevents duplicate invoice numbers for same vendor from being processed. | "Yes" in the purchasing system. "No" in the general ledger, due to the Invoice History File not being activated. | Medium |
| Unauthorized access to system, including vendor files, not adequately controlled | Access to system is password- controlled to authorized employees only. Segregation of duties is established for vendor files – only Purchasing staff can update. | Yes. | Low |
| Payment made to vendor for goods or services not received | Authorized departmental signatures are required on all invoices to document those goods or services that have been received. | Yes. | Low |
| System access capabilities not commensurate with employee job responsibilities | Employee's supervisor must authorize employee system access. | Yes. | Medium – Although supervisor approves access, one must visually ensure that the access capabilities granted are proper for the specific employee's duties. |

## Exhibit 23: Non-Quantitative Risk Assessment for Fixed Assets

| Exhibit 23: Non-Quantitative Risk Assessment for Fixed Assets | | | |
|---|---|---|---|
| **Risk** | **Control** | **Control In Place** | **Risk Assessment** |
| Recordkeeping and physical control over the movement of fixed assets (purchases, transfers, and disposals) may not be adequate. | Annual fixed asset inventory is performed by departments and overseen by the Property Control Section. In addition, Property Control performs counts and verification of assets in approximately ten departments. Established procedures are in place regarding the purchase and transfer of fixed assets. | Yes. Also, asset transactions are reconciled quarterly by agreeing system amounts to the general ledger. However, unlocated assets are sometimes noted during the annual inventory. | Medium |
| The safeguarding of assets within departments is not adequate. | Assets are tagged and accounted for on a periodic basis. | Yes. However, lost assets are identified during each annual inventory. Therefore, controls of assets at the departmental level can be considered inadequate in some instances. | Medium |
| Recordkeeping over the disposal of fixed assets may be inadequate. | Established procedures are in place regarding asset disposal including documentation and approval. | Yes, however, given that almost $12 million worth of fixed assets were disposed of in the last fiscal year, accurate and timely recordkeeping could be at risk. | Medium |

## RISK RESPONSE

**"Risk Response" is how management chooses to respond to risk: avoiding, reducing, sharing, or accepting. Management develops a set of responses to align risks with the agency's risk tolerances and risk appetite.**

For significant risks, an agency should consider potential responses from a range of response options. The following exhibit provides examples of risk responses for avoidance, sharing, reduction, and acceptance. In this section, note that "risk acceptance" is always subject to the requirement for full compliance with all applicable federal and state laws and regulations.

## Exhibit 24: Examples of Each Type of Risk Response

| Exhibit 24: Examples of Each Type of Risk Response | |
|---|---|
| **Type of Risk Response: Avoidance** | **Type of Risk Response: Sharing** |
| • Eliminating an organizational unit, service, or geographical coverage area<br>• Deciding not to engage in new initiatives or activities that give rise to risks | • Insuring significant unexpected loss<br>• Entering into joint ventures or partnerships<br>• Outsourcing business processes<br>• Sharing risk through contractual agreements with clients, vendors, or other organizations |
| **Type of Risk Response: Reduction** | **Type of Risk Response: Acceptance** |
| • Diversifying service offerings and methods<br>• Establishing operational limits<br>• Establishing effective business processes<br>• Enhancing management involvement in decision making and monitoring<br>• Reallocating funds among operating units | • "Self-insuring" against loss<br>• Relying on natural offsets within a portfolio<br>• Accepting risk as already conforming to risk tolerances |

Inherent risks are analyzed and responses evaluated with the intent of achieving a residual risk level aligned with the agency's risk tolerances. At the completion of its response actions, management may have a view of individual risks and responses and their alignment with associated tolerances, as illustrated in Exhibit 25 (next page).

## Exhibit 25: Linking Objectives, Events, Risk Assessments, and Risk Reponses

| Exhibit 25: Linking Objectives, Events, Risk Assessment, and Risk Response | | | | | |
|---|---|---|---|---|---|
| Operations objective | Hire 40 new qualified nurses across all departments to meet patient demand without overstaffing | | | | |
| Objective unit of measure | Number of new qualified staff hired | | | | |
| Tolerance | 37 – 43 new qualified nurses | | | | |
| Risks | Inherent Risk Assessment | | Risk Response | Residual Risk Assessment | |
| | Likelihood | Impact | | Likelihood | Impact |
| Decreasing number of qualified candidates available | 20% | • 10% reduction in hiring, or<br>• 4 unfilled positions | Contract in place with a third party hiring agency to source candidates | 10% | • 10% reduction in hiring, or<br>• 4 unfilled positions |
| Unacceptable variability in our hiring process | 30% | • 5% reduction in hiring, or due to poor candidate screenings<br>• 2 unfilled positions | Review of hiring process conducted every two years | 20% | • 2% reduction in hiring, or due to poor candidate screenings<br>• 1 unfilled position |
| Aligning with risk tolerance | Response expected to bring agency within risk tolerance | | | | |

Management may rely on multiple techniques to reduce the overall residual risk in order to meet its risk tolerance. The following exhibit illustrates how an agency uses multiple risk response techniques to reduce the risk of non-compliance with local environmental laws and regulations. In this example, management has not evaluated the effect of each risk response selected but has evaluated them together to establish residual risk.

## Exhibit 26: Linking Objectives, Events, Risks, and Multiple Risk Reponses

| Exhibit 26: Multiple Risk Responses | | | | | |
|---|---|---|---|---|---|
| Compliance Objective | Pesticides are used at state premises in accordance with all relevant environmental laws and regulations | | | | |
| Unit of measure | Rate of compliance | | | | |
| Target | 100% compliance | | | | |
| Risk Tolerance | 98% – 100% | | | | |
| Risks | Risks | | Inherent Risk Assessment | Risk Response | |
| | Likelihood | Likelihood | | Likelihood | Impact |
| Pesticides are sprayed in prohibited areas | Moderate | Fines, sanctions, damaged reputation | Distribution of all pesticides for use on agency grounds is coordinated through the Facilities Department<br><br>A web-based notification form is completed by all grounds persons setting out key details 72 hours before pesticides are applied<br><br>All prohibited areas are clearly marked | Low | Fines sanctions, reputation damage |

Virtually every risk response will incur some direct or indirect cost that is weighed against the benefits it creates. The initial cost to design and implement a response (processes, people, and technology) is considered, as is the cost to maintain the response on an ongoing basis. The cost, and associated benefits, can be measured quantitatively or qualitatively.

ARM requires that risk be considered from an agency-wide, or portfolio, perspective. Typically, management first considers risk for each organizational unit, department, or function, with the responsible manager developing a composite assessment of risks for the unit reflecting the unit's residual risk profile relative to its objectives and risk tolerances. Senior management is then in a good position to take an agency-wide view, to determine whether the agency's residual risk profile is commensurate with its overall risk appetite relative to its objectives. Further, management has an opportunity to reevaluate the nature and type of risk it wishes to take.

## CONTROL ACTIVITIES

**"Control Activities" are policies and procedures established and implemented to help ensure the risk responses are effectively executed. Control activities occur throughout an organization, at all levels and in all functions. They include a range of activities such as approvals, authorizations, verifications, reconciliations, security over assets, and segregation of duties.**

Management identifies control activities needed to help ensure that the selected risk responses are carried out properly and in a timely manner. Control activities should align with valid response types – avoidance, reduction, sharing, and acceptance.

- For example, to reduce the risk of the adverse effects a disruption in electrical power would have on patient care, a hospital's management decided to install a backup electricity generator. To ensure that the generator operates when needed, the facilities management department conducts routine maintenance, with maintenance logs reviewed monthly by the head of the facilities management department.

- In another example, an agency operating a large number of motor vehicles identified global oil price changes as a risk. After assessing the risk likelihood and impact and considering the agency's risk tolerance, management decided to accept the risk. Management instituted a policy whereby an agency analyst formally reassesses economists' predictions for future oil prices every three months, after which the analyst reports to the management committee its recommendations on agency and project budget adjustments.

Sometimes the control activities themselves serve as the risk response. This is frequently the case with respect to risks related to reporting objectives, as illustrated in Exhibit 27 (next page).

## Exhibit 27: Linking Objectives, Events, Risks, Reponses, and Control Activities

| Exhibit 27: Linking Objectives, Risks, Responses, and Control Activities | | | | | |
|---|---|---|---|---|---|
| Reporting Objective | Asset acquisitions and expenses incurred are entered for processing completely (C) and accurately (A), and are valid (that is, the acquisitions and expenditures occurred) (V) | | | | |
| Unit of Measure | Financial reporting errors detected, measured in dollars | | | | |
| Target | Errors in monthly financial statements typically do not occur | | | | |
| Tolerance | Errors typically not tolerated | | | | |
| Risks | Risks | | Inherent Risk Assessment | Risk Response | |
| | Likelihood | Impact | | Likelihood | Impact |
| Vendor invoices are not received prior to the year-end cutoff | Possible | Moderate $10,000-$25,000 | See below for control activities that serve as the responses to these risks | Possible | Minor ≤$2,500 |
| Vendors are paid from statements as well as invoices, causing duplicate payments | Unlikely | Minor $5,000-$15,000 | | Highly Unlikely | None expected |
| Control Activities | • Asset acquisition and expense transactions are subjected to programmed edit and validation checks:<br>○ Purchasing data (PO number, amount, etc.) are validated against tables (A)<br>○ Key fields are tested for blanks, alphas, values within a specified range (e.g., purchase amounts), missing data elements (e.g., payment due date), and programmed check digits (e.g., vendor number) (A)<br>○ Edit checks compare key amounts with tables to ensure input data are within limits established for each user or class of user (e.g., payment amounts are compared with approval limits for electronic payment) (A)<br>○ Edit checks compare vendor name, vendor number, and invoice numbers with those already paid to ensure valid vendor and to detect duplicate payments (V)<br>• All payment transactions input are matched to the original purchase order details before further processing may occur (A)<br>• Payment amounts and other details, including electronic payment transactions, are verified on screen by someone other than the staff member responsible for the original payment information (A,V)<br>• Staff reconcile each batch or series of on-line transactions with system reports (A,C)<br>• Exception reports are produced listing large or unusual items (e.g., amounts exceeding $100,000), which are then individually compared with input documents (A)<br>• Exception reports produce a listing of unmatched purchase orders open for more than 30 days for investigation (C)<br>• Changes to user-defined system parameters (e.g., authorization limits) are automatically reported and checked by an independent official (A,C,V)<br>• Users not allowed to overrides system edits (A,C,V) | | | | |

Exhibit 28 (next page) illustrates control activities that also themselves be risk responses.

## Exhibit 28: Control Activities That Serve as Risk Responses

| Exhibit 28: Control Activities That Serve as Risk Responses |
|---|
| • To ensure that pension obligations and costs are reported properly in the financial statements, management reviews the state's demographic data and the methods and assumptions used by the actuary, and compares amounts in the actuary's report with those in the financial statements and related footnotes.<br>• To help ensure that the agency's monthly income tax remittances are made in compliance with regulations, an electronic tickler file prompts staff with due dates for tax filings, and a supervisor verifies timely remittance.<br>• To help ensure that computer interfaces between general ledger systems operate to effect complete and accurate processing, transaction totals from subsidiary systems are compared with the balance in the general ledger control account, with any differences reported and followed up.<br>• To help minimize inventory losses, transfer documents are reviewed and approved by the warehouse supervisor before goods are released.<br>• To help ensure that only tested and accepted programs are transferred from test to production libraries, transfers are made only based on completion of testing and related approvals and authorization of the IT and user department managers. |

## INFORMATION AND COMMUNICATION

**"Information and Communication" involves identifying, capturing and communicating relevant information in a form and timeframe that enables people to carry out their responsibilities. Effective communication occurs down, across and up the agency. An effective information and communication process will assure that all personnel receive a clear message from top management that ARM responsibilities must be taken seriously.**

Information is needed at all levels of an agency to identify, assess, and respond to risks, and to otherwise run the agency and achieve its objectives. Information flows into, out of, and within an agency to support its ongoing management.

Technology plays a critical role in enabling the flow of information in an agency, including information directly relevant to ARM. The following exhibit illustrates information needs that management may consider when planning and implementing technological infrastructures.

## TOOLS – INFORMATION AND COMMUNICATION PLANNING

### Exhibit 29: Planning Considerations for Information Requirements

| Exhibit 29: Planning Considerations for Information Requirements |
|---|
| • What are the key performance indicators for the business?<br>• What key risk indicators provide a top-down perspective of potential risks?<br>• What performance metrics are required for monitoring?<br>• What data are required for the performance metrics?<br>• How frequently does the information need to be collected?<br>• What level of accuracy or rigor is needed?<br>• What are the criteria for data collection?<br>• Where and how should data be obtained (e.g., from organizational units or operating areas, electronically or manually)?<br>• What data are present from existing processes?<br>• How should data repositories be structured?<br>• What data recovery mechanisms are needed? |

Communications are the key to creating a healthy internal environment and to supporting the other components of ARM. Thought multiple communication channels, management reinforces or uplifts an agency's culture with both words and everyday actions. Exhibit 30 illustrates an internal communications program specifically to support the integration of its risk management philosophy and to help reinforce an ethical internal environment.

## Exhibit 30: Communicating an Agency's Risk Management Philosophy

| Exhibit 30: Communicating an Agency's Risk Management Philosophy |
|---|
| • Management discusses risks and associated risk responses in regular briefings with employees.<br>• Management regularly communicates agency-wide risks in employee communications.<br>• Agency ARM policies, standards, and procedures are made readily available to employees along with clear statements requiring compliance.<br>• Management requires employees to consult with others across the organization as appropriate when new events are identified.<br>• New hire orientation sessions include information and literature on the agency's risk management philosophy and ARM program.<br>• Tenured employees are required to take workshops or refresher courses on the agency's ARM initiatives.<br>• The risk management philosophy is reinforced in regular and ongoing internal communications programs and through specific communication programs to reinforce tenets of the agency's culture |

The following is an exhibit depicting a sample letter that the head of an agency may want to send to its employees, emphasizing the importance of ARM.

## Exhibit 31: Sample Message from the Agency Head

**Exhibit 31: Sample Message from the Agency Head**

Our overall objective is to provide essential services, protect the Commonwealth's interests, and maintain citizens' confidence.

To achieve this, we must have superior risk management capabilities that address the full spectrum of risks facing our agency and its programs. A structured and disciplined approach to risk management will minimize avoidable loss, change, and uncertainty as we reach our strategic objectives. Also, we must cope deftly with emerging risks and opportunities in an increasingly complex environment.

Each of you has a role to play in risk management. This means understanding the risks and opportunities facing our agency, assessing our exposure, and taking prompt and effective action to meet constituents' needs while safeguarding state resources from loss or inappropriate use.

We have developed a framework document – that tool that will guide our efforts to

- Manage risks, uncertainties, and opportunities,
- Support the achievement of our strategic objectives,
- Maintain full credibility and accountability, and
- Comply with applicable laws and regulations.

We look to all of our employees to apply this framework on a daily basis, and expect for you to hold agency management accountable for setting a strong and positive example.

In addition to "top-down" information flows, personnel should be able to communicate risk-based information in all directions within an agency. The following exhibit lists various methods of communication that management may use.

## Exhibit 32: Types of Communication Vehicles

| Exhibit 32: Types of Communication Vehicles |
|---|
| • Broadcast e-mails<br>• Broadcast voice mails<br>• Agency newsletters<br>• Databases supporting specific risk issues<br>• Letters from the agency head<br>• E-mail discussion groups<br>• Intranet sites capturing information regarding ARM for easy access by employees<br>• Messages integrated into ongoing agency communications<br>• Organization, function, or location-wide webcasts or conference calls<br>• Posters or signs reinforcing key aspects of ARM<br>• Regular face-to-face meetings of "risk champions" or other employees from a range of functions and organizational units with responsibility for aspects of ARM<br>• Regular risk management conference calls among a network of risk champions and other employees<br>• Regularly issued newsletters from the chief risk officer and supporting staff<br>• "Town-hall" meetings |

Many organizations use technology to facilitate ongoing ARM communication for. The next exhibit illustrates information typically provided and made readily available on a web site.

## Exhibit 33: Examples of ARM Information that an Intranet Could Provide

| Exhibit 33: Examples of ARM Information that an Intranet Could Provide |
|---|
| • "Ask anything" links<br>• Agency Head's message stating the agency's risk management philosophy, risk appetite, and basic objectives of its ARM approach<br>• Discussion forum<br>• ARM policies and procedures<br>• Frequently-asked questions regarding the agency's ARM program<br>• Relevant ARM reports and reporting activities<br>• Readily accessible information on and links to agency whistle-blower channels or hotlines<br>• Links to other organizations' websites providing information on risk management within key functions and processes, such as human resources policies, procurement, travel, vendor relations, etc.<br>• List of responsibilities and contact information for chief risk officer and key staff supporting the ARM program |

A desirable goal is, over time, to embed communications on ARM into an agency's broad-based, ongoing communications programs, consistent with the concept of building ARM into the fabric of the organization.

If regular communications channels are not effective or appropriate, an agency may set up supplemental employee communications channels. These channels, which may be called "whistle blower" programs or "ethics hotlines," may be voluntary or legally mandated. The Commonwealth presently has the legally mandated State Employee Fraud, Waste and Abuse Hotline for the use of all state employees. This does not preclude an individual agency from setting up their own hotline for their employees.

Exhibit 34 (next page) identifies items to be considered in setting up an ethics hotline.

## Exhibit 34: Considerations for Ethics Hotlines

| Exhibit 34: Considerations for Ethics Hotlines |
|---|
| • Are reporting mechanisms and protocols such that personnel will feel comfortable using the channel?<br>• What procedures will be used to ensure personnel trust the communications channel, with no concern about potential reprisal?<br>• Will the system be managed internally or by an external third party?<br>• How will incidents be prioritized?<br>• How will appropriate follow-up resources be identified?<br>• What is target response time?<br>• What are documentation standards?<br>• What monitoring processes should be in place?<br>• Are technology and security resources sufficient to manage the system?<br>• Who will perform any necessary investigations?<br>• How will complaints be documented and tracked?<br>• How will the employee reporting the information be advised of conclusions and actions taken?<br>• What kinds of summary reports are needed, and with what frequency?<br>• What mechanisms will be in place to ensure needed broad-based corrective and future preventive actions are taken? |

## MONITORING

**"Monitoring" is the process of assessing the presence and functioning of ARM components. Modifications are then made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.**

Many different activities performed in the ordinary course of running a business serve to monitor the effectiveness of ARM components. These include day-to-day review of information in carrying out normal business activities, as illustrated in Exhibit 35 (next page).

## Exhibit 35: Examples of Ongoing Monitoring Activities

| Exhibit 35: Examples of Ongoing Monitoring Activities |
|---|
| • Management reviews reports of key business activity indicators, including both key financial and operational statistics.<br>• Operating management compares production, inventory, quality measures, sales, and other information obtained in the course of daily activities to systems-generated information and to budget or plan<br>• Management reviews performance against limits established for risk exposures, such as acceptable error rates, items in suspense, reconciling items, or exposure to counterparties.<br>• Management reviews transactions reported through escalation triggers.<br>• Management reviews key performance indicators such as trends in direction and magnitude of risks, status of strategic and tactical initiatives, trends or variances in actual results to budget or prior periods, and event triggers, as described in "event identification." |

While ongoing monitoring procedures usually provide important feedback on the effectiveness of other ARM components, it may be useful to periodically evaluate directly the effectiveness of ARM. (Appendix B provides more specific tools for the evaluation process.) Evaluating ARM is a process in itself and should be adequately documented. A disciplined process provides a sound basis for an evaluation. Exhibit 36 (next page) illustrates one possible basic approach.

## Exhibit 36: Steps in an Ad Hoc Evaluation

| Exhibit 36: Steps in a Ad Hoc Evaluation |
|---|
| **Planning**<br>• Define the objectives and scope of the evaluation<br>• Identify an executive with requisite authority to manage the evaluation<br>• Identify the evaluation team, support personnel, and key organizational unit contacts<br>• Define the evaluation methodology, timeline, and steps to be conducted<br>• Agree on evaluation plan<br>**Performance**<br>• Gain an understanding of the organizational units' or processes' activities<br>• Understand how the units' or processes' risk management system is designed to work<br>• Apply the agreed-on-methods to evaluate the risk management process<br>• Analyze results by comparison to the agency's internal audit standards and follow up as necessary<br>• Document deficiencies and proposed remediation, if applicable<br>• Review and validate findings with appropriate personnel<br>**Reporting and Corrective Actions**<br>• Review results with organizational unit/process and other management as appropriate<br>• Obtain comments and remediation plans from organizational unit/process management<br>• Incorporate management feedback into final evaluation report |

A variety of evaluation methodologies and tools are available, including checklists, questionnaires, and flowcharting techniques. When selecting evaluation methodologies, determine whether they can be readily used by assigned staff, are relevant to the given scope, and are appropriate to the nature and expected frequency of the evaluation.

For example, to understand and document differences between business process design and actual performance, reviewing or developing process flowcharts and control matrices may be appropriate. When evaluating whether specific mandated control activities are present, a pre-established questionnaire may suffice. Exhibit 37 (next page) lists methodologies used, either individually or in conjunction with one another.

## METHODOLOGIES

### Exhibit 37: List of Assessment Methodologies

| Exhibit 37: List of Assessment Methodologies |
|---|
| • Process flowcharting<br>• Risk and control matrices<br>• Risk and control reference manuals<br>• Benchmarking using internal, industry, or peer information<br>• Computer assisted audit techniques<br>• Risk and control self-assessment workshops<br>• Questionnaires<br>• Facilitated sessions |

Exhibit 38 contains an excerpt of a risk and control self-assessment questionnaire for a payroll process, serving as a diagnostic reference point focusing on the extent to which controls related to payroll processing risks actually are being applied. The results form a basis for needed corrective action.

### Exhibit 38: Risk and Control Self-Assessment Questionnaire Excerpts

| Exhibit 38: Risk and Control Self-Assessment Questionnaire Excerpts | | | | | | |
|---|---|---|---|---|---|---|
| **Payroll Questions** | **Questionnaire Response Options** | | | | | **Policy Reference** |
| 1. My department reviews the budget summaries prepared by the Budgeting Department | Yes | No | Don't know | N/A | N/A | Payroll Policy 1 |
| 2. My department monitors the number of employees paid from our budget | Yes | No | Don't know | N/A | N/A | Payroll Policy 2 |
| 3. My department reviews the monthly report of salaries and wages posted to our department | Never | Seldom | Usually | Always | N/A | Payroll Policy 3 |
| 4. When reviewing this payroll report, what would you consider to be an exceedingly high number of overtime payroll hours per person that you review in detail to determine the underlying causes? | 10-20 | 20-30 | 30-40 | > 40 | Don't know | No Payroll Policy |

| Exhibit 38: Risk and Control Self-Assessment Questionnaire Excerpts |
|---|
| **Summary of Findings** |
| 95% of respondents review budget summaries prepared by the Budgeting Department |
| 93% review the number of people paid from their budget |
| 70% always review payroll reports; 18% usually do, and 12% seldom review these reports |
| 44% would review 10–20 overtime hours; 5% would review 20–30 hours; 6% would review 30–40 hours; 3% would review > 40 hours; 42% don't know |

Documentation of a state agency's ARM varies with the agency's size, complexity, and management style. In evaluating ARM, existing documentation of processes and other activities are reviewed, or may be created, to allow the evaluation team to readily understand the unit, process, or department's risks and responses. Documentation considered in an evaluation may include:

- Organization charts
- Description of key roles, authorities, and responsibilities
- Policy manuals
- Operating procedures
- Process flowcharts
- Relevant controls and associated responsibilities
- Key performance indicators
- Key identified risks
- Key risk measures

With regard to developing documentation of the evaluation process itself, the evaluation team might consider the extent to which documentation is expected to achieve the objectives of:

- Providing an audit trail of the team's assessments and testing
- Communicating evaluation results – findings, conclusions, and recommendations
- Facilitating review by supervisory personnel
- Facilitating evaluations in subsequent periods

- Identifying and reporting broader issues
- Identifying individual roles and responsibilities in the evaluation process
- Supplementing existing ARM documentation that may be deficient

All identified ARM deficiencies that affect an agency's ability to develop and implement its strategy and to set and achieve its objectives should be reported to those positioned to take necessary action. Exhibit 39 illustrates sample guidelines for reporting deficiencies.

## Exhibit 39: Illustrative Guidelines for Reporting Deficiencies

| Exhibit 39: Illustrative Guidelines for Reporting Deficiencies |
|---|
| • Deficiencies are reported to persons directly responsible for achieving business objectives affected by the deficiency.<br>• Deficiencies are reported to the person directly responsible for the activity and a person at least one level higher.<br>• Alternative reporting channels exist for reporting sensitive information such as illegal or improper acts.<br>• Specified types of deficiencies are reported to more senior management.<br>• Protocols are established for what is reported to the board of directors or a specified board committee.<br>• Information on corrective actions taken or to be taken is communicated back to relevant personnel involved in the reporting process. |

Exhibit 40 (next page) illustrates criteria for deciding which deficiencies are to be reported to senior management and maybe to the board of directors.

## Exhibit 40: Illustrative Criteria for Reporting to Senior Management

| Exhibit 40: Illustrative Criteria for Reporting to Senior Management |
|---|
| Deficiencies will be reported where the likelihood of an event occurring is not insignificant, and the impact is such that there could be a resulting:<br>• Adverse impact on safety of staff or others<br>• Illegal or improper act<br>• Significant loss of assets<br>• Failure to achieve key objectives<br>• Negative effect on the agency's reputation<br>• Improper external reporting |