AAM 05. INTERNAL CONTROLS

AAM 05.010 Background and Definition (04-14)

This section provides agency heads, managers, internal auditors, and other agency staff with a background in and approach to establishing and maintaining an effective system of internal control and internal audit so as to reasonably assure that they are meeting their respective objectives.

Background

In the United States there is common guidance on the structure of internal control systems. This is due in part to guidance issued by the American Institute of Certified Public Accountants (AICPA) and the federal Office of Management and Budget (OMB). It is also due to a 1992 report on internal control, Internal Control – Integrated Framework (Framework), issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). An addendum was published in 1994, and the Framework has remained unchanged since then.

The Framework is the national internal control standard, and AAM 5 is based on Framework guidance. In 2006, COSO published additional guidance on how to apply the Framework and in 2007 and 2008, published Guidance on Monitoring. In addition to the aforementioned COSO updates, new standards were recently adopted by the AICPA and OMB that strengthen assessment and reporting requirements for internal

controls. AAM 5 incorporates concepts from the updated COSO guidance and the new AICPA and OMB standards.

Additional information and material regarding internal controls is available through the Division of Finance web site at http://doa.alaska.gov/dof/controls.

Definition

Internal control is a process – affected by those charged with governance, management, and other personnel – designed to provide reasonable assurance about the achievement of the entity's objectives. For purposes of AAM 05, the state's objectives fall into separate but related categories:

- Safeguard its assets.
- Check the accuracy and reliability of its accounting data.
- Promote operational efficiency.
- Encourage adherence to policies for accounting and financial controls.

This definition of internal control reflects the following fundamental concepts:

- Internal control is a process. It is not one event, but a series of ongoing actions and activities that occur throughout each agency's operations and should be an integral part of each agency rather than an add-on system within an agency.
- People are what make internal control work. While the responsibility for good internal control ultimately rests with management, all agency personnel play important roles.
- No matter how well designed and operated, internal control can provide only reasonable (not absolute) assurance that all agency objectives will be met.

AAM 05.020 Responsibility (04-14)

Each agency, regardless of size, should adopt methods to periodically assess risk and to develop, implement, and review its system of internal controls. The methods should be tailored to the specific needs of the agency.

The **agency head or authorized designee** is ultimately responsible for identifying risks and establishing, maintaining, and reviewing the agency's system of internal control. If the agency head delegates this responsibility, the designated person should have sufficient authority to carry out these responsibilities. Normally, this person is a senior agency manager who does not serve in the internal audit function.

Agency management at all levels is responsible for internal control under their span of control. Management should make it clear that **agency staff** have explicit or implicit control activity duties including: delivery of services to the public; producing information for the management control system; maintaining financial information; and inspecting or maintaining physical assets. In addition, agency management should provide channels outside normal reporting lines so agency staff can report problems in operations, noncompliance with codes of conduct, violations of policy, and illegal acts.

Management is also responsible to convey the importance of internal controls to all personnel both by what they say and what they do. If management is willing to override controls, then the message that controls are not important will be conveyed to employees.

Each **agency employee** is responsible to be aware of and attentive to risk management and internal control issues, to consider limitations and key risk areas, to document decisions and to provide support information. To be most effective, employees need to understand the agency's mission, objectives, responsibilities, and their own role in managing risk. Each employee is also responsible to report to management noncompliance with codes of conduct, violations of policies, and illegal acts.

The **internal auditor or other professionals** (internal or external to the agency) may provide technical assistance in developing appropriate procedures to conduct risk assessments and internal reviews of control activities.

AAM 05.030 Framework Components (04-14)

There are five interrelated components of an internal control framework: control environment, risk assessment, control activities, information and communication, and monitoring. These components make up the minimum level of internal control an agency needs to have in place and are the basis against which internal control is evaluated.

To implement the framework, management develops the detailed policies, procedures, and practices to fit their agency's operations, and ensures that they are built into and are an integral part of operations. If an agency considers the framework components in its planning efforts and builds them into its daily processes, the agency will be poised to achieve the maximum benefit for the lowest cost.

Control Environment

The control environment of an agency sets the tone of the organization and influences the effectiveness of internal controls within the agency. The

control environment is an intangible factor. Yet, it is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment.

Management is very influential in determining the control environment and influencing the control consciousness of agency staff. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. Conversely, internal controls are likely to be ineffective if management does not believe the controls are important or if management communicates a negative view of controls to employees.

Management influences the control environment through their integrity and ethical values, commitment to competence, philosophy and operating style, design of the organizational structure, assignment of authority and responsibilities, and human resource policies and practices.

Management also influences the control environment through communication of the agency's values and behavioral standards to employees. This can be done by setting a good example, showing a positive attitude toward accounting and internal control, displaying and following a formal code of conduct, communicating other agency policies and procedures, taking swift and appropriate disciplinary action in response to policy departure, and maintaining clear and updated job descriptions.

Risk Assessment

Within the context of the state's operating environment, management sets goals and objectives at the unit and agency level that align with the agency's mission and state law. Objectives must exist before management can identify potential events affecting their achievement.

Risk assessment is the process of: identifying risks to achieving agency objectives; analyzing potential events, considering their likelihood of occurring and impact on achieving agency objectives; and deciding how to respond to the risks.

The first step is risk identification, which is the ongoing process of collecting, analyzing and adjusting information about what could happen in agency operations that would adversely affect the ability to achieve agency objectives.

To fully identify risks, both internal and external events that can affect the achievement of an agency's objectives need to be considered. Risk identification methods may include qualitative and quantitative ranking activities, forecasting, strategic planning, and consideration of findings from audits and other assessments.

Management should be aware of potential high-risk areas and should look for high risk where:

- There is a susceptibility to or history of waste, fraud, or errors.
- Changes have occurred in the organizational structure, systems, or personnel.
- Controls have not been reviewed for a substantial period of time.

The second step is analyzing the key risks for their possible effect, considering likelihood and impact. **Likelihood** is the possibility that a specific event will occur. **Impact** is the result or effect of an event.

The third step is deciding how to respond to each risk. The most common risk responses are avoiding, reducing, transferring (sharing), and accepting risk. A complete risk response should consider what actions to take and who is responsible. Refer to AAM 05.050 for more information on risk assessment.

Control Activities

Control activities help ensure risk responses are effectively carried out and include policies and procedures, manual and automated tools, approvals, authorizations, verifications, reconciliations, security over assets, and segregation of duties. These activities occur across an agency, at all levels and in all functions, and are designed to help prevent or reduce the risk that agency objectives will not be achieved.

Managers set up control activities to provide reasonable assurance that the agency and business unit objectives are met. An example of a control activity is something as simple as listing tasks assigned to staff members and then periodically checking the list to verify that assignments are completed on time. Refer to AAM 05.090 for further discussion of control activities.

Information and Communication

An agency's control structure must provide for the identification, capture and exchange of information both within the agency and with external parties. Information communicated should be timely and accurate.

Risk communication creates a dialog about the existence, nature, severity, or acceptability of risks. The identification of new risks or changes in risk is dependent on communication.

Communication can be formal through reports, training, written policy manuals, accounting and financial reporting manuals, websites, memoranda, etc. Information is also communicated informally through e-mail, speech, and actions of management and other agency personnel.

Effective **internal communication** happens when information can travel in all directions within an agency – up, down, and across. Clear internal communication conveys the agency's code of ethics, internal control philosophy and approach, and delegation of authority. Communication effectively conveys the importance and relevance of internal control and the roles each person plays to support it, including the means of reporting exceptions to an appropriate higher level within the agency.

Open **external communication** channels allow stakeholders, including citizens, clients, and suppliers, to understand the agency's service standards and provide valuable input on performance and service quality and effectiveness. This exchange enables an agency to address evolving needs, demands, and preferences. Management should appropriately convert such input into continuous improvements in operations, reporting, and compliance.

Monitoring

Things change and, by monitoring the risks and the effectiveness of control measures on a regular basis, an agency can react dynamically to changing conditions.

Monitoring evaluates the effectiveness of an agency's internal controls and is designed to ensure that internal controls continue to operate effectively. Monitoring is effective when it leads to the identification and correction of control weaknesses *before* they **materially** affect the achievement of the agency's objectives.

An agency's internal control is most effective when there is proper monitoring, results are prioritized and communicated, and weaknesses are corrected and followed up on as necessary.

There are two types of monitoring: ongoing and periodic. Ongoing monitoring occurs in the course of operations. It includes tasks such as supervisory reviews of reconciliations, reports, and processes. Periodic monitoring includes tasks such as periodic internal audit sampling and annual reviews of high-risk business processes. Internal control deficiencies uncovered by monitoring should be reported to higher levels of management.

AAM 05.040 Annual Requirements for Agencies (04-14)

Annual Assurance

The departments should annually determine if internal control modifications are needed by considering events that have occurred, processes or procedures that have changed, new projects or programs that are being planned or implemented, and other changes within the agency

that may have additional risks. If the review uncovers internal control weaknesses or if prior weaknesses still exist, they should be documented and addressed.

Periodically, an agency should conduct a comprehensive review of the internal control structure to determine if it is adequately addressing agency risks. This can be done agency-wide at one time or by sections of the agency over a period of time.

Agencies must maintain adequate written documentation of activities conducted in connection with risk assessments, review of internal control activities and follow-up actions. This documentation includes any checklists and methods used to complete these activities. Please see the sample checklists that are available through the Division of Finance web site at http://doa.alaska.gov/dof/controls. Refer AAM 05.130 for required documentation.

Agencies have the flexibility to assign appropriate staff to complete the risk assessments and review of internal control activities required by this policy. The assigned staff provides assurance to the agency head that the agency has performed the required risk assessments and the necessary evaluative processes. This communication may be ongoing and informal, but **at least once per year**, this assurance must **be made in writing** to the agency head.

The assigned staff is responsible for ensuring that the required documentation is maintained and available for review by agency management.

Annual Reporting

The Department of Administration, Division of Finance distributes an annual internal control acknowledgement letter that is signed by the designated officials. This acknowledgement provides the Division of Finance with reasonable assurance that controls are in place at the departments.

By signing the acknowledgement of internal control responsibility the individuals certify that:

- Management acknowledges their responsibility that internal control processes have been established and followed within the department and that the agency's system of internal controls complies with the requirements of AAM 05.
- Management has identified the requirements governing the services that the department provides and is responsible for the department's compliance with applicable state and federal laws and regulations.

- Management has reviewed the accounts receivable recorded in the statewide financial system for the department and deems them to be collectible.
- There is no known noncompliance with state and federal requirements within the department that could have a material effect on the determination of financial statement amounts that have not been disclosed.
- Employees are adequately trained and/or supervised.
- Instances of fraud involving management and/or employees have been reported to the Director of the Division of Finance. All suspected misuse of state credit cards should be reported to the agency's human resource manager and Labor Relations. The human resource manager will investigate, coordinating with the agency and the Division of Finance. (AAM 38.325)
- Material financial transactions have been properly recorded within the State's financial system.
- Assets of the department are properly safeguarded against loss from unauthorized use or disposition.
- Any related party transactions have been properly disclosed to the Division of Finance. Related parties include members (or their family) of the governing body, board members, or administrative officials with influence over the department. Transactions between the department and these individuals, or which are less than "arms-length" for other reasons, would be considered related party transactions.

AAM 05.050 Risk Assessment (04-14)

Risk assessment is an ongoing process that includes identifying risks to achieving agency objectives, analyzing the risks, and deciding how to respond to the risks.

In risk assessment, management considers the mix of potential events relevant to the agency and its activities in the context of the agency's public visibility, size, operational complexity, regulatory restraints, and other factors. Because of these variables, the same activity could have very different levels of risk for two different agencies.

AAM 05.060 Risk Identification (04-14)

Risk identification is the first step in risk assessment because risk cannot be measured, prioritized, and managed until it has been identified. Every agency faces a variety of risks, both expected and unexpected, from external and internal sources that must be identified.

External risks arise from activities outside the agency. These external risks may not be directly controllable by the agency or they may constrain the way in which the agency is permitted to take or address risk. Technological developments, changing public expectations, legislative directives, natural catastrophes and economic changes all have the potential for creating external risks in an agency.

Internal risks arise from activities inside the agency. Examples of internal risks include disruption of the central computer system or telephone system and turnover in a key managerial position.

The process of identifying risks should consider the following characteristics and attributes: type of risk, source of risk, areas the risk impacts, and level of ability to control the risk.

Risk identification can often be integrated into the planning activities that occur at various levels within the agency. Some risks may be apparent at the agency level, whereas others may be a factor only within a certain function or process. Risks at all levels should be identified and aggregated across the agency. The significant ones will become apparent during the risk analysis process.

Risks can also be identified through ongoing activities. The budget process, audits, and the strategic planning process provide opportunities for managers to conduct quantitative and qualitative reviews and to identify risks. More informal opportunities include senior management planning meetings, meetings with auditors, and everyday interaction with staff.

More important than the specific method used to identify risks is management's careful consideration of factors unique to the agency, including the following:

- An agency's past experience.
- Staffing levels and quality.
- Statutory framework.
- The significance and complexity of activities in relation to the agency's mission.

Tools related to risk identification and assessment are available online through the Division of Finance web site at http://doa.alaska.gov/dof/controls.

Once risks have been identified, they need to be analyzed. This analysis includes estimating the impact of a risk, measuring the likelihood it will occur, and considering how to respond to the risk.

Analysis of the Control Environment

Analyzing risk begins with analyzing the control environment. The control environment is the foundation for all other components of internal control. Refer to AAM 05.030 for a discussion of the control environment.

Analysis of Inherent Risk

Analyzing risk also includes analyzing the inherent risk. High inherent risk is not necessarily a reflection of management performance or lack of control; rather, high inherent risk points to areas that, due to the nature of their operations, require additional attention. For example, from a safeguarding of assets perspective, activities involving the handling of cash are inherently more risky than activities involving the handling of sand and gravel. However, from a financial reporting perspective, the measuring of cash is inherently less risky than measuring sand and gravel.

Other Factors that Influence Risk

Other factors may influence risk measurement. These factors can be grouped into broad categories such as:

- Financial
- Operational
- Human capital
- Legal
- Technology
- Security
- Political
- Environmental
- Ethics
- Compliance

The degree to which these factors influence a specific agency or function will vary depending on the agency's objectives, the nature of its operations and its control environment.

Measuring Risk

A visual matrix can be useful in measuring risk. For each event, determine the likelihood that it will occur and the impact on the agency if it does occur.

- **Likelihood** = the possibility that a given event will occur.
- **Impact** = the result or effect of an event.

	Low Impact	Medium Impact	High Impact
High Likelihood	2	3	3
Medium Likelihood	1	2	3
Low Likelihood	1	1	2

A general guideline for handling the different levels of risk is:

- 3 = High Risk – Mitigate or reduce the risks
- 2 = Medium Risk – Manage the risks
- 1 = Low Risk – Accept the risks

The specific method used to measure risk is not as important as ensuring that management gives careful consideration to factors unique to their agency and that the risk assessment process is well documented.

AAM 05.080 Response to Risk (04-14)

Risk response refers to the actions taken to deal with an identified risk. Possible responses fall into four categories: avoidance, reduction, transferring (sharing), and acceptance.

Avoidance

Risk avoidance involves eliminating the risk-producing activity entirely (or never beginning it). Although avoidance is highly effective, it is often impractical or undesirable, either because the agency is legally required to engage in the activity or because the activity is so beneficial to the public that it cannot be discontinued.

Reduction

Risk reduction strategies reduce the frequency or severity of the losses resulting from a risk, usually by changing operations. For example, routine mechanical maintenance could decrease the likelihood of a major computer hardware failure, while routine backups could decrease the

impact of technology equipment failure on the agency's ability to provide services.

Transferring (sharing)

Risk transfer strategies turn over or share the responsibility of performing a risky activity to another party. Examples of risk transfer are transferring the liability for losses to an insurance carrier, or outsourcing an activity to a contractor with the stipulation that the contractor assume the risk.

Acceptance

After all reasonable and cost-effective risk responses have been taken, an agency is left with risk acceptance.

When deciding how to respond to each risk, management should consider the following:

- The availability and effectiveness of control activities on likelihood and impact (significance).
- The availability of resources to implement control activities.
- The cost of the control activity in relation to its benefit.

Limitations on resources will define the way and level to which risks can be managed. Therefore, risk responses must be prioritized based on level of risk and the cost, availability, and effectiveness of control activities.

When considering the cost versus benefit and recognizing interrelationships among risks, management may pool agency responses to address similar risks across an agency's units or programs. Examples include mandating ethics training for all agency employees and centralizing functions, such as contract management and receipting.

AAM 05.090 Control Activities (04-14)

Control activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out. In other words, control activities are **actions taken** to minimize risk. The need for a control activity is established in the risk assessment process. When the assessment identifies a significant risk to the achievement of an agency's objective, a corresponding control activity or activities is determined and implemented.

Control activities can be preventive or detective:

Preventive activities are designed to deter the occurrence of an undesirable event. The development of these controls involves predicting

potential problems before they occur and implementing procedures to avoid them.

Detective activities are designed to identify undesirable events that do occur and alert management about what has happened. This enables management to take corrective action promptly.

Internal control activities can be incorporated into the following:

- Policies
- Procedures
- Sequences or combinations of procedures
- Assignments of duties, responsibilities, and authorities
- Physical arrangements or processes
- Combinations of the above

AAM 05.100 Internal Control Plan (04-14)

Control activities occur at all levels and functions of the agency. Management should establish control activities that are effective and efficient. While designing and implementing control activities, management should aim to get the maximum benefit at the lowest possible cost. Consideration should be given to the following:

- The cost of the control activity should not exceed the cost that would be incurred by the agency if the undesirable event occurred.
- Management should build control activities into business processes and systems as the processes and systems are being designed.
- Adding control activities after the development of a process or system is generally more costly.
- The allocation of resources among control activities should be based on the likelihood and impact of the risk. Refer to AAM 05.030.
- For any given risk, there may be multiple appropriate control activities that can be put into place, either individually or in combination with other control activities.
- Excessive use of controls could impede productivity.

AAM 05.110 Commonly Used Control Activities (04-14)

The following are descriptions of some commonly used control activities. This is not an exhaustive listing of the alternatives available to management.

Authorization

Control activities in this category are designed to provide reasonable assurance that all transactions are within the limits set by policy or that exceptions to policy have been granted by the appropriate officials.

Review and Approval

Control activities in this category are designed to provide reasonable assurance that transactions have been reviewed for accuracy and completeness by appropriate personnel.

Verification

Control activities in this category include a variety of computer and manual controls designed to provide reasonable assurance that all accounting information has been correctly captured.

Reconciliation

Control activities in this category are designed to provide reasonable assurance of the accuracy of financial records through the periodic comparison of source documents to data recorded in accounting information systems.

Physical Security Over Assets

Control activities in this category are designed to provide reasonable assurance that assets are safeguarded and protected from loss or damage due to accident, natural disaster, negligence or intentional acts of fraud, theft or abuse.

Segregation of Duties

Control activities in this category reduce the risk of error and fraud by requiring that more than one person is involved in completing a particular fiscal process.

Education, Training and Coaching

Control activities in this category reduce the risk of error and inefficiency in operations by ensuring that personnel have the proper education and training to perform their duties effectively. Education and training programs should be periodically reviewed and updated to conform to any changes in the agency environment or fiscal processing procedures.

Performance Planning and Evaluation

Control activities in this category establish key performance indicators for the agency that may be used to identify unexpected results or unusual

trends in data which could indicate situations that require further investigation and/or corrective actions. Evaluations may be done at multiple levels within the agency, as appropriate: the agency as a whole; major initiatives; specific functions; or specific activities.

Performance reviews may focus on compliance, financial or operational issues. For example, financial reviews should be made of actual performance versus budgets, forecasts and performance in prior periods.

Although control activity procedures are not intended to increase staffing levels, acceptable procedures are to be established and followed which may require changes in existing workloads and staff assignments.

However, a periodic thorough internal review of control activities may identify policies and procedures that are no longer required. It is recognized that some small to medium size operations may not be able to institute internal control procedures on the same level as larger, more complex agencies. In those cases where staffing may prohibit or restrict the appropriate segregation of duties, management must either have more active oversight of operations or utilize personnel from other units to the extent possible as compensating controls.

AAM 05.120 Control Activity Limitations (04-14)

Control activities, no matter how well designed and executed, can provide only **reasonable assurance** regarding achievement of objectives. The likelihood of achievement is affected by limitations inherent in all control systems. These limitations include the following:

Judgment

The effectiveness of controls will be limited by the fact that decisions must be made with human judgment in the time available, based on information at hand and under the pressures to conduct business.

Breakdowns

Even if control activities are well designed, they can break down. Personnel may misunderstand instructions or simply make mistakes. Errors may also stem from new technology and the complexity of computerized information systems.

Management Override

Even in an effectively controlled agency, high-level personnel may be able to override prescribed policies or procedures for personal gain or advantage. This should not be confused with management intervention,

which represents management actions to depart from prescribed policies or procedures for legitimate purposes.

Collusion

Collusion between two or more individuals can result in control failures. Individuals acting collectively often can alter financial data or other management information in a manner that cannot be identified by the control system.

Costs versus Benefit

In determining whether a particular control activity should be established, the cost of establishing the control must be considered along with the risk of failure and the potential impact. Excessive control is costly and counterproductive. Too little control presents undue risk. Agencies should make a conscious effort to strike an appropriate balance.

Resource Limitations

Every agency must prioritize control activities because resources are not available to put every control activity into practice.

AAM 05.130 Internal Control Documentation (04-14)

Documentation involves preserving evidence that substantiates a decision, event, transaction or system. Documentation should be complete, accurate and clearly written. It should be recorded timely and in a format that can be used efficiently.

At a minimum, documentation should be retained of the following:

- Key policies, procedures and processes.
- The annual assurance required in AAM 05.040.

Agencies should strive to develop documentation of its processes that includes:

- The control objective as related to a desired goal or condition.
- The flow of information and documents through the process or function.
- The control activities in place over the function.

Documentation should be considered in making decisions about the internal controls in place over a specific process. The documentation should be sufficient to allow the agency to:

- Conclude as to the overall soundness of the internal controls.

- Be aware of the existence of internal control weaknesses, if any.
- Formulate the agency's plan of action for addressing internal control weaknesses and improving the internal controls where necessary.

AAM 05.140 Loss of Public Funds or Property (04-14)

In the event of the suspected loss of public funds or property, it is important that correct procedures are followed in order to:

- Minimize the loss.
- Ensure that investigations are not hampered.
- Ensure that extravagant settlements are not made.
- Ensure that bond claims are not jeopardized.
- Ensure that incorrect personnel actions are not taken.

AAM 05.150 Suspicion of Loss (04-14)

Each agency should establish formal notification procedures to notify appropriate agency personnel when someone suspects a loss of public funds or property. Appropriate personnel not involved in the suspected loss should be notified prior to contacting outside agencies. This may include the agency head or deputies, chief financial officer or internal auditor depending upon the circumstances.

Per AS 37.10.090, whenever money, funds, or property of a city, school district, municipal government, or the state are illegally paid or are diverted for an illegal purpose, or paid to a person not authorized by law to receive them, they may be recovered by an action instituted by the attorney general.

The agency's Assistant Attorney General should be consulted on incidents involving the suspected loss of public funds or property. It is best to establish general procedures to follow upon learning of a suspected loss of public funds or property. In addition, it may be appropriate to contact local or state law enforcement officials.

Protect any pertinent records, regardless of format (i.e., paper, electronic, etc.), from destruction or manipulation.