Revised 3/31/2010

CHAPTER 6.

MANAGER'S RESPONSIBILITY FOR INTERNAL CONTROLS

SECTIONS

6-01 PURPOSE

This chapter prescribes policy and procedures and assigns responsibilities for establishing and maintaining adequate systems of internal controls in the programs and activities of the National Oceanic Atmospheric Administration (NOAA). The provisions of this chapter apply to all program, financial, and administrative activities of NOAA.

6-02 AUTHORITY

This chapter is issued pursuant to the following authorities:

- Federal Managers' Financial Integrity Act (FMFIA) of 1982 (31 U.S.C. 3512)
- OMB Circular A-123, Management's Responsibility for Internal Control
- GAO Standards for Internal Controls in the Federal Government
- GAO Internal Control Management and Evaluation Tool
- Chief Financial Officers Act (P.L. 101-576)

- Government Performance and Results Act (GPRA) (P.L. 103-62)
- Department of Commerce Guidelines for Conducting Non-Financial Internal Control Reviews

6-03 RESPONSIBILITY

NOAA management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. NOAA management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness.

6-04 INTERNAL CONTROL STANDARDS

Internal control, in the broadest sense, includes the plan of organization, methods and procedures adopted by management to meet its goals. Internal control includes processes for planning, organizing, directing, controlling, and reporting on NOAA operations. The three objectives of internal control are:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

The safeguarding of assets is a subset of all of these objectives. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use or disposition of assets.

NOAA management is responsible for developing and maintaining internal control activities that comply with the following standards to meet the above objectives:

- Control Environment,
- Risk Assessment,
- Control Activities,
- Information and Communications, and
- Monitoring `

A. Control Environment
The control environment is the NOAA organizational structure and culture created by management and employees to sustain organizational support for effective internal control. When designing, evaluating or modifying organizational structure, management must clearly demonstrate its commitment to competence in the workplace. Within the NOAA organizational structure, management must clearly:

- define areas of authority and responsibility,

- appropriately delegate the authority and responsibility throughout NOAA,
- establish a suitable hierarchy for reporting,
- support appropriate human capital policies for hiring, training, evaluating, counseling, advancing, compensating and disciplining personnel,
- uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties and to understand the importance of maintaining effective internal control within NOAA.

The NOAA organizational culture should be defined by management's leadership in setting values of integrity and ethical behavior but is also affected by the relationship between NOAA, central oversight agencies, and Congress. Management's philosophy and operational style will set the tone within NOAA. Management's commitment to establishing and maintaining effective internal control should cascade down and permeate NOAA's control environment which will aid in the successful implementation of internal control systems.

B. Risk Assessment

NOAA management should identify internal and external risks that may prevent NOAA from meeting its objectives. When identifying risks, management should take into account relevant interactions within NOAA as well as with outside organizations. Management should also consider previous findings; e.g., auditor identified, internal management reviews, or noncompliance with laws and regulations when identifying risks. Identified risks should then be analyzed for their potential effect or impact on NOAA. See *Risk Assessment Template* at http://www.rdc.noaa.gov/~finance/Risk Assessment Template.xls for suggested format.

C. Control Activities

Control activities include policies, procedures and mechanisms in place to help ensure that NOAA's objectives are met. Several examples include:

- proper segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction);
- physical controls over assets (limited access to inventories or equipment);
- proper authorization; and
- appropriate documentation and access to that documentation.

Internal control also needs to be in place over information systems – general and application control. General control applies to all information systems such as the mainframe, network and end-user environments, and includes NOAA-wide security program planning, management, control over data center operations, system software acquisition and maintenance. Application control should be designed to ensure that transactions are properly authorized and processed accurately and that the data is valid and complete. Controls should be established at an application's interfaces to verify inputs and outputs, such as edit checks. General and application control over information systems are interrelated, both are needed to ensure complete and accurate information processing. Due to the rapid changes in information technology, controls must also adjust to remain effective.

D. Information and Communications
Information should be communicated to relevant personnel at all levels within NOAA. The information should be relevant, reliable, and timely. It is also crucial that NOAA communicate with outside organizations as well, whether providing information or receiving it. Examples include: receiving updated guidance from central oversight agencies; management communicating requirements to the operational staff; operational staff communicating with the information systems staff to modify application software to extract data requested in the guidance.

E. Monitoring
Monitoring the effectiveness of internal control should occur in the normal course of business. In addition, periodic reviews, reconciliations or comparisons of data should be included as part of the regular assigned duties of personnel. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in NOAA's operations. If an effective continuous monitoring program is in place, it can level the resources needed to maintain effective internal controls throughout the year.

F. Deficiencies
Deficiencies found in internal control should be reported to the appropriate personnel and management responsible for that area. Deficiencies identified, whether through internal review or by an external audit, should be evaluated and corrected. A systematic process should be in place for addressing deficiencies.

NOAA managers and staff should be encouraged to identify control deficiencies, as this reflects positively on NOAA's commitment to recognizing and addressing internal control problems. Failing to report a known reportable condition would reflect adversely on NOAA and continue to place NOAA's operations at risk. NOAA managers should carefully consider whether systemic weaknesses exist that adversely affect internal controls across organizational or program lines.

6-05 CONTROL ACTIVITIES

Internal control activities are the policies, procedures, techniques, and mechanisms that help ensure that management's directives to mitigate risks identified during the risk assessment process are carried out. Control activities are an integral part of NOAA's planning, implementing, and reviewing. They are essential for proper stewardship and accountability for government resources and for achieving effective and efficient program results.

Control activities occur at all levels and functions of NOAA. They include a wide range of diverse activities, such as approvals, authorizations, verifications, reconciliations,

performance reviews, security activities, and the production of records and documentation. A manager or evaluator should focus on control activities in the context of NOAA's management directives to address risks associated with established objectives for each significant activity (program or mission). Therefore, a manager or evaluator will consider whether control activities relate to the risk-assessment process and whether they are appropriate to ensure that management's directives are carried out. In assessing the adequacy of internal control activities, a reviewer should consider whether the proper control activities have been established, whether they are sufficient in number, and the degree to which those activities are operating effectively. This should be done for each significant activity. This analysis and evaluation should also include controls over computerized information systems. A manager or evaluator should consider not only whether established control activities are relevant to the risk-assessment process, but also whether they are being applied properly.

A. General Control Activities

There are several general control activities that are applicable throughout NOAA, including:

1. Appropriate policies, procedures, techniques, and mechanisms exist with respect to each of NOAA's activities.

2. The control activities identified as necessary are in place and being applied. For example:

    - Control activities described in policy and procedures manuals are actually applied and applied properly.

    - Supervisors and employees understand the purpose of internal control activities.

    - Supervisory personnel review the functioning of established control activities and remain alert for instances in which excessive control activities should be streamlined.

    - Timely action is taken on exceptions, implementation problems, or information that requires follow-up.

3. Control activities are regularly evaluated to ensure that they are still appropriate and working as intended.

4. Management tracks major NOAA achievements in relation to its plans.

5. NOAA managers review actual performance against targets.

6. NOAA effectively manages NOAA's workforce to achieve results.

7. NOAA employs a variety of control activities suited to information processing systems to ensure accuracy and completeness.

8. NOAA employs physical control to secure and safeguard vulnerable assets. For example:

    - Physical safeguarding policies and procedures have been developed, implemented, and communicated to all employees.

    - Assets that are particularly vulnerable to loss, theft, damage, or unauthorized use, such as cash, securities, supplies, inventories, and equipment, are physically secured and access to them controlled.

9. NOAA has established and monitors performance measures and indicators. For example:

    - Performance measures and indicators have been established throughout NOAA at the NOAA-wide, activity, and individual level.

    - Performance measurement assessment factors are evaluated to ensure they are linked to mission, goals, and objectives, and are balanced and set appropriate incentives for achieving goals while complying with law, regulations, and ethical standards.

    - Actual performance data are continually compared against expected/planned goals and differences are analyzed.

10. Key duties and responsibilities are divided or segregated among different people to reduce the risk of error, waste, or fraud. For example:

    - No one individual is allowed to control all key aspects of a transaction or event.

    - Responsibilities and duties involving transactions and events are separated among different employees with respect to authorization, approval, processing and recording, making payments or receiving funds, review and auditing, and the custodial functions and handling of related assets.

    - NOAA management is aware that collusion can reduce or destroy the control effectiveness of segregation of duties and, therefore, is especially alert for it and attempts to reduce the opportunities for it to occur.

11. Transactions and other significant events are authorized and performed by the appropriate personnel. For example:

- Controls are established to ensure that all transactions and other significant events that are entered into are authorized and executed only by employees acting within the scope of their authority.

12. Transactions and other significant events are properly classified and promptly recorded. For example:

    - Transactions and events are appropriately classified and promptly recorded so that they maintain their relevance, value, and usefulness to NOAA management in controlling operations and making decisions.

    - Proper classification and recording take place throughout the entire life cycle of each transaction or event, including authorization, initiation, processing, and final classification in summary records.

13. Access to resources and records is limited and accountability for their custody is assigned.

14. Internal control and all transactions and other significant events are clearly documented. For example:

    - The documentation is readily available for examination.

    - Documentation, whether in paper or electronic form, is useful to managers in monitoring their operations and to any others involved in evaluating or analyzing operations.

    - All documentation and records are properly managed, maintained, and periodically updated.

B. Information System Control Activities

In addition, there are some control activity factors specifically designed for information systems. As discussed previously, there are two broad groupings of information systems control: general control and application control.

General control includes the structure, policies, and procedures that apply to NOAA's overall computer operations. It applies to all information systems, mainframe, mini-computer, network, and end-user environments. General control creates the environment in which NOAA's application systems operate. The general control activities include:

1. NOAA periodically performs a comprehensive, high-level assessment of risks to its information systems.

2. NOAA has developed a plan that clearly describes the NOAA-wide security program and policies and procedures that support it.

3. NOAA senior management has established a structure to implement and manage the security program throughout NOAA, and security responsibilities are clearly defined.

4. NOAA has implemented effective security-related personnel policies.

5. NOAA monitors the security program's effectiveness and makes changes as needed.

6. NOAA classifies information resources according to their criticality and sensitivity.

7. Resource owners have identified authorized users, and their access to the information has been formally authorized.

8. NOAA has established physical and logical controls to prevent or detect unauthorized access.

9. NOAA monitors information systems access, investigates apparent violations, and takes appropriate remedial and disciplinary action.

10. Information system processing features and program modifications are properly authorized.

11. All new or revised software is thoroughly tested and approved.

12. NOAA has established procedures to ensure control of its software libraries, including labeling, access restrictions, and use of inventories and separate libraries.

13. NOAA limits access to system software based on job responsibilities, and access authorization is documented.

14. Access to and use of system software is controlled and monitored.

15. NOAA controls changes made to the system software.

16. Incompatible duties have been identified and policies implemented to segregate those duties.

17. Access controls have been established to enforce segregation of duties.

18. NOAA exercises control over personnel activities through the use of formal operating procedures, supervision, and review.

19. The criticality and sensitivity of computerized operations have been assessed and prioritized, and supporting resources have been identified.

20. NOAA has taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures including offsite storage of

21. NOAA management has developed and documented a comprehensive contingency plan.

22. NOAA periodically tests the contingency plan and adjusts it as appropriate.

Application control covers the structure, policies, and procedures designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. It includes both the routines contained within the computer program code as well as the policies and procedures associated with user activities, such as manual measures performed by the user to determine that the data were processed accurately by the computer. The application control activities include:

1. Source documents are controlled and require authorization.

2. Data entry terminals have restricted access.

3. Master files and exception reporting are used to ensure that all data processed are authorized.

4. All authorized transactions are entered into and processed by the computer.

5. Reconciliations are performed to verify data completeness.

6. NOAA's data entry design features contribute to data accuracy.

7. Data validation and editing are performed to identify erroneous data.

8. Erroneous data are captured, reported, investigated, and promptly corrected.

9. Output reports are reviewed to help maintain data accuracy and validity.

10. Procedures ensure that the current version of production programs and data files are used during processing.

11. Programs include routines to verify that the proper version of the computer file is used during processing.

12. Programs include routines for checking internal file header labels before processing.

13. The application protects against concurrent file updates.

Additional information on control activities can be found in GAO publication GAO-01-1008G, Internal Control Management and Evaluation Tool, which is available at http://www.gao.gov/new.items/d011008g.pdf.

6-06 MANAGEMENT CONTROL REVIEW

Each NOAA Line and Staff Office is responsible for conducting a Management Control Review at least annually.

The purpose of a Management Control Review is to evaluate the management controls of a specific activity and determine how well they promote good management. Additionally, the review will help your office operate more efficiently and effectively, and to provide a reasonable level of assurance that the process and products for which you are responsible are adequately protected.

Internal controls are processes designed to provide reasonable assurance about the achievement of the entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over the safeguarding of assets against unauthorized acquisition, use, or disposition may include controls related to financial reporting and operations objectives. Generally, controls that are relevant to an audit of financial statements are those that pertain to the entity's objective of reliable financial reporting.

The steps Management Control Review consists of: 1) Conducting a Risk Assessment, 2) Reviewing Internal Controls, 3) Report Findings, and 4) Monitoring.

The purpose of a risk assessment is to determine an area of vulnerability that could be subject to waste, loss, unauthorized use, or misappropriation.

- Conduct a risk assessment to determine an area of concern within your office that has a high risk of inadequate controls. (Use Attachment A for format.)

Explanations for Columns on Risk Assessment Forms:

Assessable Unit - An organizational subdivision capable of being evaluated by control review procedures. An assessable unit should be a subdivision of an organization that ensures a reasonable span of internal control to allow for meaningful control analysis.

Identifying the Event Cycle(s) for Review

The assessable unit is the focus of evaluative work in the internal control process. To properly plan the scope of an internal control review, the review team must understand the activities and responsibilities of the assessable unit as a whole. This may be accomplished through a review of mission statements, Department Administrative Orders, Department Organization Orders, briefing books, and budget justifications;

through interviews; or by relying on other sources that describe the work that takes place within the assessable unit.

The MCR need not concentrate on all parts of the assessable unit. Consequently, an assessable unit may be subdivided into smaller functional groupings called event cycles. Each event cycle has a distinct starting point and ending point, and is cyclical in nature. When combined, event cycles reflect all work that is performed within the assessable unit. Care should be taken to examine an entire event cycle – rather than portions of it.

It may be helpful to consider the results or end products that an assessable unit is responsible for achieving and then examining the process used to do so. Particular attention should be given to programs that have large appropriations, are subject to specific managerial concern, have previously identified control problems, are inherently high risk, are highly sensitive or visible, or have not been recently reviewed – through an internal control review or otherwise. If event cycles seem to be of equal importance, the event cycle(s) which affects the greatest level of funding or has the most important control implications should be reviewed.

Documentation: Attachment B, "List of Event Cycles," may be used to identify and prioritize event cycles for review.

OIG and GAO Reports or Actions – These columns indicate recent monitoring activity by the indicated agencies, going back five years. Monitoring by outside parties reduces the risk that a significant control weakness may go undetected.

PART Ratings – PART assessments are broad-based and may not impact risk assessment consistently across all assessable units in an evaluated program area. Generally, a "Performing" rating indicates a decrease in risk, while a "Not Performing" rating indicates an increase.

Substantial Management Responsibility Outside NOAA – These programs pass significant funding, and consequently significant management responsibility, through to parties outside the Federal government. This could increase the risk of a weakness in management controls.

Substantial Change in Recommended Funding – Significant increases or decreases in program funding can put pressures on management, possibly increasing risk.

Substantial Change in Performance Measure – A change in a performance measure can place additional pressures on management, increases the possibility of control weakness.

Overall Results of Risk Assessment – This column summarizes the assessment of relative risk for the listed assessable units.

Documentation: Complete Risk Assessment Template.

Reviewing Internal Controls

In general, an internal control review consists of:

- selecting a team to conduct the review,
- planning the internal control review,
- investigating and reviewing background material,
- documenting the event cycle,
- analyzing the control environment,
- determining risks within the selected event cycle(s),
- developing control objectives,
- identifying existing control techniques,
- testing internal control techniques, and
- evaluating internal controls.

Selecting the Internal Control Review Team

The number of team members depends on the scope and complexity of the internal control review. Team members should have some analytical background, expertise in planning and conducting studies, and experience in preparing written reports.

Each member should already be or become familiar with the concept of internal controls, and the requirements of an internal control review. At least one team member should be a subject matter specialist in the functional area being examined. If possible, for greater objectivity, one member should be selected from outside the event cycle(s) being examined. To be even more beneficial, this team member could be a specialist in an administrative area that may be of particular significance to the area under review, e.g., information technology, budget, accounting, or travel.

Assessable unit managers should select an internal control review team capable of providing a meaningful assessment in a reasonable time frame.

Documentation: Each team member's name, title, organization, address, telephone number and relevant experience should be listed in an appendix to the internal control review report.

Planning the Internal Control Review

After the internal control review team has determined which event cycle(s) will be reviewed, a plan for conducting the internal control review should be prepared. In developing the review plan, realistic time frames should be established.

Documentation: The review plan should provide information similar to Attachment C, "Internal Control Review Plan."

Investigating and Reviewing Background Material

This section outlines the procedure for defining the process or work flow that constitutes the event cycle, and sets the stage for the internal control review team to identify controls within that process. After the event cycle(s) has been selected, team members should familiarize themselves with the process being examined and the environment in which it exists. This investigation will be more complete than the relatively general investigation initially undertaken to determine the event cycles within the assessable unit. The investigation will focus directly on the event cycle(s) selected for review and should be quite detailed. Examples of documents that should be reviewed at this stage include:

- enabling legislation and implementing regulations;
- government-wide and Commerce policy guidance;
- operating unit directives;
- program-specific operating policies and procedures;
- mission statements;
- annual and strategic plans;
- performance measures, including measures established under the Government Performance and Results Act;
- delegations of authority;
- existing flowcharts;
- budget, personnel, and workload data;
- organizational charts;
- forms used in the process;
- position descriptions;
- vulnerability assessments, management reports, and issue papers; and
- other recent studies.

Throughout this review, the focus of attention should be on documenting and evaluating internal controls that exist within the selected event cycle(s).

The review of background information should be augmented by interviews with relevant employees, as necessary. Interviews should be conducted to help clarify the process within the event cycle and to support the information gathered through initial research. Employees who are directly involved in or responsible for daily operations should be selectively interviewed to assist in developing a valid flowchart of the process(es).

Interview questions should be developed in advance, and should give the manager or staff member an opportunity to explain operations and discuss any perceived problems. Questions should cover the process as well as formal and informal controls that are in place.

Documentation: Narrative description of items reviewed.

Documenting the Event Cycle(s)

Based on its review of relevant background information, the internal control review team should then prepare a narrative description of the work that takes place and a flowchart. These documents will provide a firm basis for a structured examination of controls within the event cycle(s).

Using knowledge gained from the background investigation, the study team should prepare a short narrative description of each step, in sequence; that occurs within the process under review. The description of each step may be only a few words; the important aspect of this exercise is to make sure that each significant phase of the process is identified. Generally, the work flow includes an input, a processing phase, and an output.

The description should incorporate all work that is performed within the event cycle. The team should determine the significant action that initiates the process and the action that concludes the process. After these boundaries have been established, the remaining steps will become more readily apparent. The description should identify the employees involved, the forms that are used and their points of distribution, reviews and approvals that take place, the physical location of the activity, and any similar information that will help clarify the process. Once the narrative description has been completed, a flowchart may be developed for the process.

After the review team feels comfortable with the flowchart, its accuracy should be verified with operational managers or other personnel involved in carrying out the work.

Documentation: Narrative description and flowchart. The flowchart should provide information similar to Attachment D, "MCR Flowchart Example."

Analyzing the Control Environment

The environment in which an event cycle operates has a major impact on the effectiveness of its internal control system. Poor training, ineffective communications, or lack of properly delegated authority, as examples, may negate the effectiveness of even the best control system. Therefore, an analysis of the control environment is an important phase of an internal control review.

This portion of the review should consider:

- Organization Structure
- Personnel
- Delegation of Authority and Responsibility
- Policies and Procedures
- Planning, Budgeting, and Reporting
- Organizational Checks and Balances

Complete Attachment E, "Evaluation of General Control Environment" for template.

If deficiencies are identified, they should be noted, along with recommendations for improvements, as part of the overall evaluation of management controls. (See Attachment F, "Evaluation of Management Controls," for a sample template.)

Documentation: Narrative description of the control environment that discusses each of the areas listed above.

Determining Risks Within the Event Cycle(s)

Determining risks that exist within the event cycle(s) will be one of the most critical phases of the internal control review; control systems are intended to avoid potential risks.

All administrative and program areas have some degree of risk -- a negative event or situation -- that would occur if all or a part of the process under review is not carried out as planned. In this phase, the internal control review team must determine what risks exist, evaluate the nature and magnitude of their potential impact, and determine who, both inside and outside of the organization, could be affected. Each risk identified will describe an event or situation that the organization wishes to avoid.

Risks should be identified without considering controls that may be in place. Even if the internal control review team believes that existing controls adequately address a given risk, it should still be identified and examined. By doing so, the team will objectively confirm the existence of good management practices within the event cycle and cover all significant risks in the review.

Since each event cycle is different, unique controls are needed to counteract risks that exist within individual event cycles. Risks that are considered during an internal control review are not only those related strictly to potential fraud, waste, abuse and mismanagement but also factors that could impede the proper conduct of normal, daily operations. The internal control team must consider the risks associated with failing to properly carry out the event cycle's operational responsibilities. Reviews of this nature concentrate on promoting good management practices within event cycles and collectively improve the Department's overall management processes over time. Therefore, determining risks means identifying:

- the consequence of not performing, as intended, each step of the process identified during the flowcharting phase; and
- any unique risks associated with the event cycle(s), specific safety and security considerations, or the ramifications of not complying with program legislation or regulatory mandates.

Examples of risks that may occur in an event cycle include:

- mishandling sensitive or classified documents, which could have significant security implications;

- inadequate competition during a procurement transaction, which could result in unnecessarily wasting financial resources;
- failure to adhere to budgetary plans, which could result in an Antideficiency Act violation; and
- inaccurate or unreliable research data, which may have a major impact on private sector activities.

The internal control review team, in conjunction with the assessable unit manager, must make a realistic determination regarding potential risks within the process under review, and recognize the associated impact of each risk. By definition, each step that has been included in the flowchart has some level of importance in the process, and some safeguard(s) should be in place to help assure that each step is completed as intended.

After the list of risks has been fully developed, it should be reviewed by the assessable unit manager. The manager should assure that historic or current concerns have been identified.

Documentation: Identification of each risk in a format similar to Attachment G, "Event Cycle Risks, Control Objectives, and Control Techniques."

Developing Control Objectives

Simply stated, control objectives will be the opposite of the risks that have been identified – they are conditions that you want to occur. Control objectives developed in this phase of the internal control review will be used as a point of reference in identifying and evaluating control techniques. Therefore, control objectives should be complete, clearly defined, and, to the extent possible, measurable.

Realistically, event cycles should have a series of control objectives. If only one objective seems to cover all risks, either the event cycle has been defined too narrowly and does not cover the full process, or all risks have not been identified. Each identified risk must have a corresponding control objective.

Documentation: Identification of control objectives for each risk determined. (See Attachment G as a sample template.)

Identifying Existing Control Techniques

Control techniques are the safeguards put in place to assure that operations proceed according to plan and are protected from fraud, waste, abuse, and other risks. Effective control techniques allow the assessable unit manager to feel confident that their responsibilities are being carried out properly.

Control techniques are the action items in the control process. Each event cycle will likely have many control techniques, or safeguards, already in place. Because most controls are so closely associated with an event cycle, managers may have difficulty in

conceptually separating the control techniques from the process itself. Some common examples of control techniques include:

- standardized forms to collect information,
- written program procedures,
- routine schedules for equipment maintenance,
- annual inventories of personal property,
- financial planning,
- objective criteria for selecting applicants for federal benefits,
- log books,
- site visits to financial assistance recipients,
- approval procedures and signature requirements,
- eligibility criteria for program participation,
- receipts that document financial transactions,
- computer passwords to protect information technology resources,
- quality and timeliness standards for service provision,
- background checks for personnel recruitment,
- adequate supervision of staff activity,
- peer review of research proposals,
- training programs to maintain skills needed to carry out program objectives,
- security precautions in developing sensitive data prior to its formal release, and
- examining equipment purchases prior accepting delivery.

When developing control techniques, the internal control review team must address each control objective that has been identified. Each control objective may have several control techniques associated with it. The flowchart that was developed earlier will assist the review team in systematically identifying various control techniques that exist within the event cycle(s).

Documentation: Identification of control techniques to meet the control objectives determined earlier and avoid the risks identified. (See Attachment G for a sample template.)

Testing Internal Control Techniques

Employees may not be aware of a control technique or its importance, or may not have adequate time to complete the control action. Without proper support and emphasis by management, control systems will deteriorate over time. The testing phase of the internal control review will either confirm that controls are in place and operating as intended, or will point out areas where improvements may be needed in the control system.

Once existing internal control techniques have been identified, the review team must determine if they are being used routinely and if they are achieving the stated objectives. The internal control review team will use a structured testing exercise to make this determination. Testing will focus on whether the control techniques exist and are being

used. It should not focus on the procedural aspects of event cycle as described in the flowchart; rather, testing should focus on written requirements and actions that are routinely performed to make sure that operations proceed as intended.

As an example, a control technique may be "purchase orders may be processed only if they contain an approved authorizing signature." The review team would examine a representative sample of purchase orders to determine if they reflect an appropriate authorizing signature. As another example, a headquarters program may "perform semiannual monitoring visits." The internal control test would be to formally verify if these monitoring visits took place every six months, and if the visits were consistent with pre-established criteria designed for the review. An internal control test would not include actually performing the semiannual review at a field location.

Testing may be performed by using one of the general standard sampling methods; statistical or non-statistical (judgmental). Statistical sampling techniques scientifically determine the sample size and the evaluation of sample results. A recommended software for statistical sampling is www.auditnet.org/docs/statsamp.xls. You would then choose "Calc Sample Size - Attributes". Then enter your total population size and use sampling error of 5%, confidence level of 95%, and expected error rate of 3% for the highest level of confidence that your sample size is appropriate. Non-statistical sampling techniques determine the sample size and the evaluation of sample results judgmentally. A judgmental sample size should give you the maximum coverage possible of the total population. The sample size should include at least 20% of the total dollars or total line items in the population. In either case, the test must be planned in advance, test results recorded, and test data maintained for future review. Attachment H, "Testing Plan," provides a sample format for recording information that should be retained for each test.

The exact number of items that must be examined will depend on (a) the universe or total number of items that the team could potentially test, (b) the importance of the control technique, and (c) the available resources. Enough testing should be conducted to allow a reasonable degree of confidence that the results are accurate; and in line with the relative importance of the control action. If a fairly limited number of tests are performed and the results do not establish whether or not the technique is being used, an increased level of testing may be warranted. Ultimately, the amount of testing completed during an internal control review will depend on the study team's judgment.

If field activity is included in the event cycle, adequate testing of controls in the field must be accomplished. To the extent possible, this testing should be combined with other trips to field locations. This may be done by planning ahead to take advantage of previously scheduled visits. Another option would be to have an employee in the field participate in the internal control review team and perform the testing at the field site.

Documentation: For each control objective, identify the control technique, type of test, universe of potential tests, and number actually selected for review in a format similar to Attachment H.

The general objective of testing controls is to obtain reasonable assurance that the controls are in use and operating as planned. Tests should meet GAO Standards as follows:

(See http://www.gao.gov/special.pubs/ai2131.pdf for complete GAO Standards)

- Data Integrity
- Documentation
- Recordation
- Supervision
- Authorization
- Separation of Duties
- Security

Data Integrity

- Are there controls in place to ensure the integrity of the data?
- Are records up-to-date and accurate?

Documentation

- Are all systems, functions, processes, procedures, programs, and activities clearly documented?
- Is the documentation readily available for examination?
- Are operating procedures adequate?

Recordation

- Are these records that show that controls are in use?

Supervision

- Are appropriate procedures in place for assigning, reviewing, and approving work?
- Do the employees adhere to procedures for assigning, reviewing, and approving work?

Authorization

- Are appropriate controls in place to ensure transactions and other significant activities are authorized and executed only by authorized personnel?
- Do employees adhere to the requirements of authorization only by authorized personnel?

Separation of Duties

- Are key duties and responsibilities such as authorizing, processing, recording, and reviewing separated among individuals?

Security

- Are appropriate procedures in place, which limit access to resources and records to authorized personnel?
- Do employees adhere to security procedures?

Evaluating Internal Controls

After the general control environment has been defined, and existing controls have been identified and their usage tested, the control system must be evaluated. Even if the general control environment is satisfactory and existing control techniques are being used, the internal control review team cannot necessarily conclude that the existing control system is adequate. It must be evaluated to make sure that the best system possible is in place, given existing resources, to counteract existing risks. In other words, the internal control review team must consider how well the control system fosters good management. Are there too many, or perhaps, too few controls?

The relative importance of each objective should correspond with the controls that are put in place. If a control objective must be met, the control techniques employed should be developed accordingly. However, absolute or near absolute assurance is seldom required. Before control techniques are put in place to bring about absolute assurance that an objective will be met, the costs and relative benefits must be carefully considered. As control systems approach absolute assurance, they become quite time consuming and expensive. A manager may have nearly complete confidence in their control system, but the necessary cost or processing time may be unreasonable. Controls are intended to make sure that operational plans are met without substantially reducing efficiency.

The internal control review process should allow the study team to step back and objectively evaluate the controls that exist within the assessable unit, and to determine if they meet the managerial needs of the unit. This evaluation should include an assessment of the level of control associated with each objective and whether the existing control techniques actually promote compliance with the objective. Are safeguards at the right spots? Do they work or is the action superfluous?

The review team should evaluate each control objective separately. Will the control techniques currently in place provide a reasonable level of confidence that the objective will be met? If not, the review team should recommend additional or different control techniques to improve the control system and address any identified control weakness. These recommendations should be included in the final report and, when implemented, will allow the assessable unit manager to feel more confident that their operational responsibilities will be effectively met.

Documentation: A short description of the evaluation process, which should include: (a) whether the current control techniques provide an adequate level of confidence that the control objectives will be met, (b) a list of the major strengths and weaknesses in the control system, and (c) a list of recommendations to strengthen the control system or correct the weaknesses noted during this evaluation. (See Attachment F for a suggested format.)

Problems Outside the Control of the Assessable Unit Manager

An internal control review provides a good opportunity to surface control problems that may exist between the assessable unit and other government operations, i.e., intra-agency or interagency activity. If another organization is reducing the effectiveness of the event cycle's system of control, this fact should be recognized. An appropriate recommendation should be developed to address the problem, e.g., formally informing a service provider in writing of a specific concern and proposing a resolution designed to be – to the extent possible – mutually agreeable. The assessable unit manager may not have the authority to alter the other organization's operations, but should be able to initiate a dialogue to resolve the problem or raise it to a higher organizational level so that some concrete action will result.

The recommendation included in the final report should be the action that the assessable unit manager will take, not simply a description of the change that another organization may need to make. Since the assessable unit manager is most familiar with the problem, they are in the best position to describe it, explain the desired corrective measures, and carry their cause through to fruition.

3) Report Findings

When determining the severity of any findings, you must understand the 2007 definitions for material weaknesses and reportable conditions.

(See http://www.aicpa.org/download/members/div/auditstd/AU-00325.PDF for complete details.)

The definitions are as follows:

Material Weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

Significant Deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliability in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

Control Deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

The major change in definitions is findings that were once considered a reportable condition, may now be elevated to a *Significant Deficiency* or a *Material Weakness*.

Reporting the Results of an Internal Control Review

The final report is the method used to communicate the findings of the internal control review and document how it was performed. It should be remembered that the report may be reviewed by individuals with limited knowledge of the assessable unit's technical operations and should be understandable by a broad audience.

Generally, the report should include:

- Introduction – Identify the report as being the result of an internal control review and provide a short description of the review's objective. Also include a description of the assessable unit, i.e., funding, number of full-time-equivalent employees (FTE), organizational location, and functional responsibilities. The report should explain the reason that the assessable unit was chosen for review within your operating unit, program, or organizational area.

- Scope – Describe the event cycles existing within the assessable unit, which one(s) was targeted for review, and the reason for its selection. For each event cycle reviewed, provide the number of FTE, total budget, input, process, and output associated with it as well as the event cycle's significance to the mission of the organization. Briefly mention other Departmental or government organizations that may be involved in the process and their roles.

- Methodology – Briefly describe how the internal control review was conducted, addressing the various steps outlined in these guidelines and the actions taken during each step. This section should also describe the resources (FTE and funding) used to undertake the review as well as any unique problems that may have been encountered.

- General Control Environment – Include a factual discussion of each aspect of the general control environment, e.g., "the organization chart and position descriptions were updated during a June 2005 reorganization."

- Findings and Conclusions – Present the results of the internal control review in this section. The findings and conclusions should highlight both the control weaknesses and strengths found in the event cycle(s). In addition, any significant concerns or problems that were identified during the review should be discussed. In conclusion, the report should include a statement regarding whether there is "reasonable assurance" that controls are in place and operating effectively within the event cycle(s).

- Recommendations – Describe all deficiencies and associated corrective actions that

are recommended by the internal control review team and assessable unit manager. Each recommendation should be discussed individually, identifying the official responsible for implementation and the targeted completion date. Recommendations may be referenced in the narrative and discussed at length using a format similar to Attachment F.

Recommendations such as "improve monitoring – ongoing" lack specificity and are not adequate. Recommendations should be concise, clearly described, and have a definite completion date, such as "issue new procedures to improve loan monitoring by July 2007."

- Appendices should include:

  - information regarding the internal control review team members,
  - the flow chart and narrative description of the event cycle, and
  - documentation of the steps taken using matrices such as those attached to these guidelines.

Documentation: Internal control review final report. The MCR final report becomes part of NOAA's annual FMFIA report to the Secretary of Commerce. The MCR must be completed by June 30 with a final report completed by July 31 of each year.

Submitting the Management Control Review Report

Internal control review reports should be reviewed and approved by the assessable unit manager, and forwarded for review and concurrence by the program or Line Office, Chief Financial Officer or the Staff Office, Director. The assessable unit manager shall maintain working papers that support the findings and recommendations made in the report, e.g., interview records and testing records.

The original signed final version of the MCR is to be sent to the Financial Policy and Compliance Division no later than July 31. This should be sent to the attention of Nancy M. Gates, Chief, Financial Policy and Compliance Division, 20200 Century Blvd., Suite 1310, Germantown, MD 20874. Additionally, a copy of the signed report is to be sent to the Line Office, Chief Financial Officer or the Staff Office, Director.

4) Monitoring

- Resolution of Review Findings and Other Deficiencies
- Quarterly reporting of the progress of the corrective actions.

Resolution of Review Findings and Other Deficiencies – All Line/Staff Offices must develop corrective actions plans using Attachment I, "Corrective Action Template", for any finding and deficiencies and submit to the Financial Policy and Compliance Division with the report.

Quarterly Reporting of Corrective Actions – Quarterly progress reports for all corrective action plans are due to the Financial Policy and Compliance Division by the 15th day following the end of a quarter. Corrective action plans must be completed by June 30 of the following year.

6-07 CORRECTING INTERNAL CONTROL DEFICIENCIES

NOAA policy is to develop corrective action plans for all deficiencies that resulted from Management Control Reviews and other internal control reviews conducted by the NOAA Finance Office. NOAA Line and Staff Offices are required to routinely report on the progress against their plans.

Additionally, NOAA's policy for the resolution and corrective action of identified material weaknesses in internal control requires:

- NOAA managers are responsible for taking prompt and effective action to correct deficiencies identified.
- Maintain accurate records of the status of the identified material weaknesses through the entire process of resolution and corrective action.
- Assure that the corrective action plans are consistent with laws, regulations, and Administration policy.
- Assure that performance appraisals of appropriate officials reflect effectiveness in resolving or implementing corrective action for identified material weaknesses.

A determination that a reportable condition has been corrected will be made only when sufficient corrective actions have been taken and the desired results achieved.

6-08 EFFECT ON OTHER ISSUANCES

None.

6-09 APPENDIX A – RISK ASSESSMENT

See *Risk Assessment Template* at http://www.rdc.noaa.gov/~finance/Internal%20Controls.html for suggested format.

6-10 APPENDIX B

Internal Control Review
List of Event Cycles

Component/Program: _____

Assessable Unit: _____

Event Cycle	Scheduled for Review	Comment / Rationale

Prepared by: _____ Date: _____

Reviewed by: _____ Date: _____

6-11 APPENDIX C

Internal Control Review Plan

Component/Program: _____

Assessable Unit: _____

Event Cycle: _____

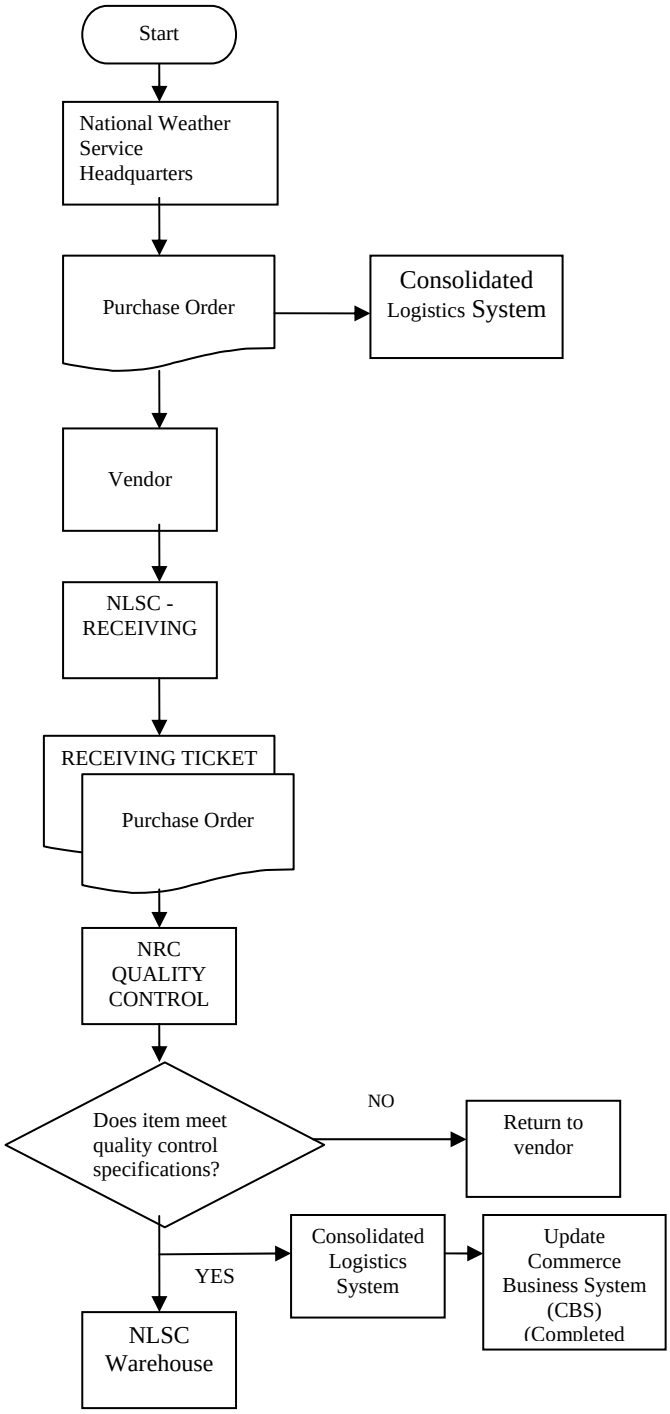
Task	Estimated Time	Start Date	End Date
1. Investigation / Review of Background Material			
2. Documentation of Event Cycle a. Narrative b. Flowchart			
3. Analysis of General Control Environment			
4. Determine Risks			
5. Develop Control Objectives			
6. Determine Control Techniques			
7. Test Control Techniques			
8. Evaluate Internal Controls			
9. Write Report			

Prepared by: _____ Date: _____
Internal Control Review Team Leader

Reviewed by: _____ Date: _____
Assessable Unit Manager

6-12 APPENDIX D

MCR Flowchart Example



6-13 APPENDIX E

Internal Control Review
Evaluation of General Control Environment

Question	Yes	No	Comments
Organization Structure:			
1. Is the organization chart current and are reporting relationships clear? (Include copy of organization chart.)			
2. Are employee responsibilities clearly divided so as to avoid duplication, overlap, or conflict?			
3. Does the organizational structure foster the achievement of the assessable unit's objectives?			
4. Are mission statements accurate and consistent with the organizational structure?			
Personnel:			
5. Are position descriptions in writing, current and consistent with mission statements?			
6. Do all employees have accurate and up-to-date performance standards?			
7. Are there periodic performance reviews and counseling for all employees?			
8. Are there sufficient training opportunities to meet competency requirements and ensure that the assessable unit's mission is achieved?			
Delegation of Authority and Responsibility:			
9. Are all appropriate delegations current, in writing and systematically maintained in a single location?			
10. Do assigned responsibilities properly reflect separation of duties, e.g., time and attendance clerks do not approve their own time sheet?			

Policies and Procedures: 11. Are policies and procedures current and in writing?			
12. Are policies and procedures clearly stated and systematically communicated (manuals, handbooks, directives, etc.)?			
13. Are policies and procedures flexible enough to accommodate unusual circumstances?			
Planning, Budgeting, and Reporting: 14. Are activities formally planned?			
15. Are reports on the activities of the event cycle timely, accurate and relevant?			
16. Is actual performance tracked and compared with (a) planned performance, (b) budget allowances, and/or (c) past performance?			
17. Are performance measures in place, as appropriate? Are they clearly defined? Is adequate documentation supporting results maintained and readily available?			
Organizational Checks and Balances: 18. Are there clearly established levels of operational and financial accountability?			
19. Are employees accountable only for matters within their control?			

Prepared by: _____ Date: _____
Internal Control Review Team Leader

Reviewed by: _____ Date: _____
Assessable Unit Manager

6-14 APPENDIX F

Internal Control Review
Evaluation of Management Controls

Component/Program: _____

Assessable Unit: _____

Event Cycle: _____

Control Objective	Are Controls Adequate?		Recommendation	Responsible Official	Target Completion Date
	Yes	No			

Prepared by: _____ Date: _____
Internal Control Review Team Leader

Reviewed by: _____ Date: _____
Assessable Unit Manager

6-15 APPENDIX G

Internal Control Review
Event Cycle Risks, Control Objectives, and Control Techniques

Component/Program: _____

Assessable Unit: _____

Event Cycle: _____

Risk	Control Objective	Control Technique

Prepared by: _____ Date: _____
Internal Control Review Team Leader

Reviewed by: _____ Date: _____
Assessable Unit Manager

6-16 APPENDIX H

Internal Control Review
Testing Plan

Component/Program: _____

Assessable Unit: _____

Event Cycle: _____

Control Objective	Control Technique	Type of Test	Universe of Potential Tests	Number Selected for Review

Prepared by: _____ Date: _____
Internal Control Review Team Leader

Reviewed by: _____ Date: _____
Assessable Unit Manager

6-17 APPENDIX I

Internal Control Review
Corrective Action Template

INTERNAL CONTROL DEFICIENCY	CORRECTIVE ACTIONS TO BE TAKEN	RESPONSIBLE PARTY AND PHONE NUMBER	ESTIMATED COMPLETION DATE	PERCENTAGE OF COMPLETION	ACTUAL COMPLETION DATE
1.					
2.					
3.					
4.					
5.					
6.					