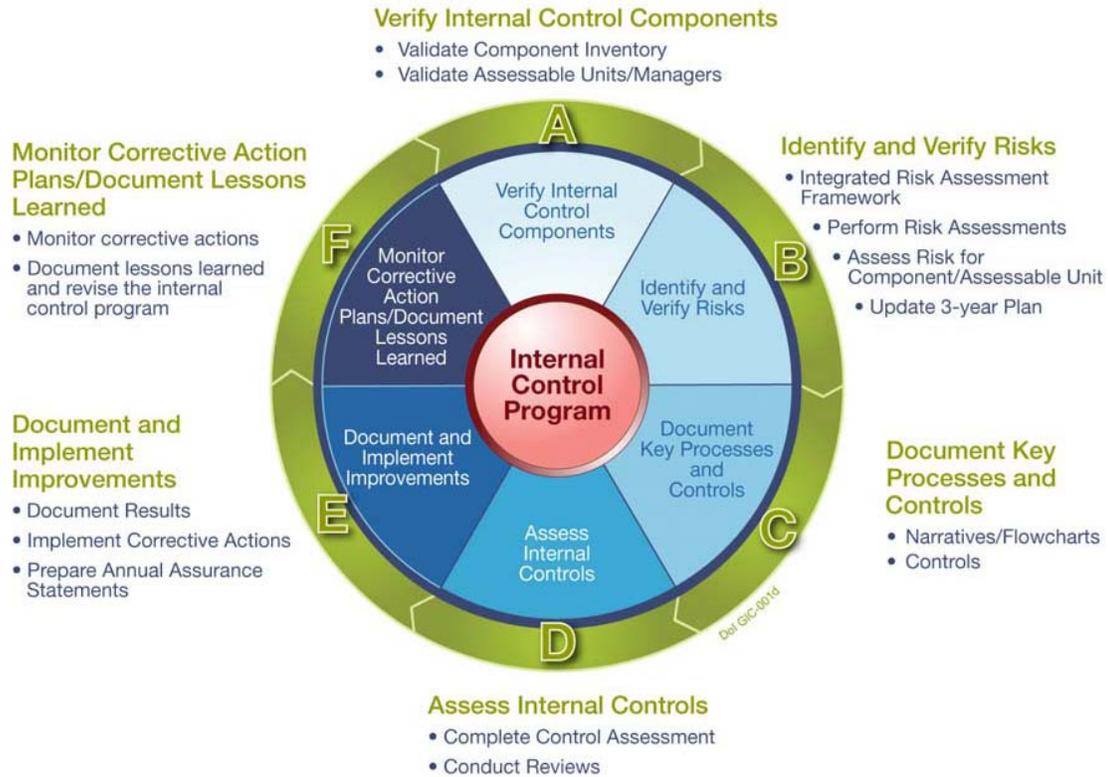


# **Internal Control Review Handbook**



**FY 2010**

**The Internal Control Review Process:**



**What is *Internal Control*?**

Internal control is a process, effected by people, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

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

Internal control is the process where policy, procedures, training, and other measures are designed to offset risks and ensure that the mission of that organization is achieved. Management actions include processes for planning, organizing, directing, controlling, and reporting on agency operations. Management has a fundamental responsibility set the tone, or the “**Control Environment**” and to develop and maintain effective internal controls to ensure proper stewardship of Federal resources, operate programs efficiently and effectively, and comply with laws and regulations.

**What is the *Control Environment*?**

An important factor to consider when assessing your internal controls is the “*Control Environment*.” The control environment is the tone of the organization largely in regard to ethics and ethical behavior. Management’s attitude, actions and values set the tone of an organization, influencing the control consciousness of its people. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. Management must also have a commitment to competence that includes a commitment to hire, train, and retain qualified staff. This commitment to competence encompasses both technical competence and ethical commitment. Management’s commitment to competence includes both hiring staff with the necessary skills and knowledge and ensuring that current staff receives adequate on-going training and supervision.

### **Why am I conducting an *Internal Control Review*?**

You conduct Internal Control Reviews (ICRs) to make sure that the controls you have in place are working. We conduct ICRs based on risk. Someone in your organization reviewed your program and rated your risk based on a number of different factors. Additionally, ICRs of programs are required under OMB Circular A-123.

### **How do we assess our Internal Controls over programs?**

First you must identify your mission or missions within your division or branch. The mission is accomplished through a series of specific *business processes* that when performed, allows for accomplishing the mission(s) of your division. These business processes are normally outlined in regulation and directives or other similar written guidance. *Key business processes* relate directly to accomplishing mission objectives (e.g. for Law Enforcement a key business process is weapons training and certification). Key business processes make up the activities that support our programs and enable mission accomplishment.

### **So what do I do once I’ve identified my key business processes?**

Assessable unit managers, or those that have been delegated the duty of performing the Internal Control Review (ICR), must identify their key business processes. Once key business processes are identified, they must be described in detail in order to perform an in-depth control analysis. This analysis will uncover the risks and controls associated with those processes. The vehicle most suited to process analysis is a detailed narrative and a business process flowchart. The Department has mandated that we flowchart our key processes as part of the FY2010 Internal Control Reviews.

### ***Key Concept: the two types of Risk you must understand:***

In order to evaluate your key processes and identify your key controls you need to understand the concept of risk. There are three types of risk you must understand to perform an ICR.

*Inherent Risk* is basic risk to accomplishing your mission. This risk can be anything from the weather, the budget, environmental contamination, or human capital. The important fact to remember about *Inherent Risk* is that it is unmitigated by any application of a control. So this is an unfettered risk.

*Control Risk* is the risk that a control will fail to offset or prevent a risk to a program objective or a process. If the *Control Risk* is high that means that the *Control* is likely to NOT mitigate the risk that it is intended to offset.

**I've never written a process narrative or flowcharted a process before. How do I begin?**

You write a narrative of your processes so you can then flowchart them. (Remember to focus in on your Key Processes.) The narratives should be of sufficient clarity to ensure that a reader will understand the detailed process. As you begin describing these processes, or tasks, you'll also have to think about what could go wrong in performing these tasks that would impede or preclude you from being successful. These are risks. They should be documented to coincide with the process they are associated with. Then consider what policy, procedures, training or tools such as a database to track activities that aid in ensuring that these risks don't thwart your efforts. These are controls.

**So what should I include in my narrative?**

Use this as a guide in preparing your narrative(s).

Narrative:

1. Does the process narrative have the preparer's name?
2. Is the process owner's name evident on the process narrative?
3. Is the process explained well in the narrative?
4. Does every step identified in the process have an associated description in the narrative?
5. Are the steps in the narrative numbered to facilitate the flowcharting process?
6. Does the narrative indicate what laws and regulations are being complied with in the process?
7. Does the narrative describe the process objectives and detail the steps required to achieve the objectives successfully?
8. Does the narrative identify and describe risks associated to the process?
9. Does the narrative identify controls?

As you document your processes you should number these processes, the risks to accomplishing these tasks, and the controls over these risks. Here is a short example:

Process 1

(Subprocess 1)

Risk 1.1

Control 1.1.1;

Process 2

Risk 2.1

Control 2.1.1

Control 2.1.2

Risk 2.2

Control 2.2.1

Control 2.2.2 etc...

Using a numbering system like this will enable you to create process flowcharts in an efficient way to document the key processes, risk(s) associated with those processes, and key internal controls (see **attachment 1** for a full narrative that uses this process).

**You say I have to determine *Inherent Risks* when I'm writing my narrative – how do I do that?**

Here is a step by step process to determine risk for a specific process:

1. Review the Risk Assessment performed for your “assessable unit” or program earlier in the year. Most if not all of your risks should be identified on your risk assessment documentation.
2. Assemble employees who perform the task(s) that make this process successful and employees who are impacted by the process to obtain diverse viewpoints. This group may include financial and IT support staff.
3. Make a list of possible things that could go wrong with the process by answering the following questions (**remember that most of the risks and many of your controls have already been identified in your risk assessment**):
  - a) What are the major objectives or initiatives for this program?
  - b) Within those objectives/initiatives what are some of the factors potentially affecting:
    - i) Accomplishment of the program (e.g. lack of funding, personnel retirements, the bridge collapses, the animal becomes extinct, etc.)?
    - ii) Efficiency of program expenditures? (e.g. what could cause your unit costs to be high? Does rework exist as an integral part of a process? Does equipment break down regularly?)
    - iii) Consistency with legal and regulatory requirements?
    - iv) Fraud, waste and abuse in the program?
    - v) Data integrity and security?

**I've identified my key business processes, risks, and controls and described them in a narrative, now what?**

Once you've identified your key processes through a narrative you will then flowchart those processes. (See **attachment 2** for an example of a partially completed flowchart that uses the previous example of the narrative and for an example of a completed flow chart see **attachment 2a**).

The following questions should be addressed in preparing flowcharts.

Flowchart:

1. Is there a defined start symbol (either start or connector from another flowchart)?
2. Is each shape in the flowchart appropriate (e.g., database reference shows a database shape)?
3. Are processes, risks, and control points numbered (use the numbers established in the narrative)?
4. Does the process end at the end of the flowchart? Is there a defined end symbol?
5. Is the next process connector on the flowchart instead of an end symbol?

6. Does the end-of-the-process describe the relationship of how the operational process outputs manifested (e.g. fuel reduction accomplished, decreased impact of wildland fire, etc...).
7. If process flowchart is linked to/from another, is the naming convention understandable and logical?

Final narratives or flowcharts should identify operational points of contact and include their names, phone numbers and email addresses. A footer with the name of the division or branch should be on each page of the process description.

The narrative and related flowchart must be at a level of detail sufficient to guide you in conducting your ICR. These products should list your risks and the controls associated with those risks. These products will also be very useful in the future for anyone who is given the task of conducting an ICR for your program or assessable unit.

### **So now that I've identified my processes, the risks and the controls what do I do with all that?**

Your next step is to document the risks, controls, and the outcome of testing those controls. To do this the Department has supplied an Excel work book specifically for this purpose (**attachment 3**). The workbook is a very easy way to document the results of all of your work. The forms are linked together and when you add data to one form pertinent pieces will carry over to other forms.

The first "form" you fill out is the *Risk Analysis Form* in the workbook. To do this you will need to perform a quick risk analysis of the inherent risks you've identified in your narrative/flowcharting process. (Your original Risk Analysis has an "Inherent Risk Rating" for risks that were identified earlier if you used the Integrated Risk Rating Tool.) You'll also have to do an initial Control Risk assessment.

### **How do I determine my level of *Inherent Risk* to my processes?**

Remember that *Inherent risk* includes conditions or events that exist, or may exist, assuming no controls are in place. Here is a simple way to determine inherent risk:

Step by step process to determine Inherent risk:

1. For each risk listed in your narrative or flowchart using professional judgment, determine the likelihood or probability of this occurring during the next twelve months?
2. For each risk listed in your narrative or flowchart, using professional judgment, determine the effect (or magnitude) on the program if the event occurred.
3. Determine the risks using the chart below to determine the risk rating for each potential event or risk.

Likelihood	Consequences				
	Insignificant (Minor problem easily handled by normal day to day processes )	Minor (Some disruption possible, e.g. damage equal to \$500k )	Moderate (Significant time/resources required, e.g. damage equal to \$1million)	Major (Operations severely damaged, e.g. damage equal to \$10 million )	Catastrophic (Business survival is at risk damage equal to \$25 Million)
Almost certain (e.g. >90% chance)	High	High	Extreme	Extreme	Extreme
Likely (e.g. between 50% and 90% chance)	Moderate	High	High	Extreme	Extreme
Moderate (e.g. between 10% and 50% chance)	Low	Moderate	High	Extreme	Extreme
Unlikely (e.g. between 3% and 10% chance)	Low	Low	Moderate	High	Extreme
Rare (e.g. <3% chance)	Low	Low	Moderate	High	High

Now that I’ve calculated my inherent risk what do I do with that information? You will use this when you list your risks on the *Risk Analysis Form* during your documenting of the ICR (**attachment 3**).

**OK – I’ve entered my *Inherent Risk* calculation on the appropriate form. What is my next step?**

Next you’ll evaluate your *Control Risk*. Remember, as discussed earlier, *Control Risk* is the risk that your controls will not mitigate the risk they were designed to control. This is an initial evaluation of your *Control Risk* based on knowledge of subject matter experts and possibly some low level testing of the controls such as samples of data, interviewing employees or observation of work being performed. For example, your program tracks progress repairing facilities in a database of deferred maintenance (this is a control). You review that database to see when it was last updated to check if people are following instructions to update status at the end of each week. You confirm that there are numerous updates for the on-going projects you are tracking. In this instance you can say that your *Control* is working and you have a low *Control Risk*.

To assess *Control Risk*:

*Control Risk*: The probability that *Control(s)* in place will fail to mitigate an inherent risk that would result in an inability to achieve operational or mission objective. The use of management’s professional judgment is essential in assessing *Control Risk*.

- Low Control Risk: The preparer believes that the control, as designed and operating WILL prevent or detect any inherent risk conditions that could occur that would significantly impact achieving operational objectives.
- Moderate Control Risk: The preparer believes that the control, as designed and operating, will MORE LIKELY THAN NOT prevent or detect any inherent risk conditions that could occur that would significantly impact achieving operational objective.
- High Control Risk: The preparer believes that controls will PROBABLY NOT prevent or detect any inherent risk conditions that could occur that would significantly impact achieving operational objectives.

**So what do I do with my Control Risk rating?**

Enter the *Control Risk* rating in the “Preliminary Control Risk” column of the Risk Analysis Form (**attachment 3**) of the Excel workbook.

**What’s my next step?**

Next you’ll go to the *Control Assessment Form* in the excel workbook. Here you’ll document the assessment of your controls. You’ll already have the controls identified on the *Risk Analysis Form* transferred over to this form. On this form you will document your evaluation of what Controls are in place and whether they are effective. You will need to test a sample of these Controls to see if they accomplish the intended purpose.

**How do I perform Control Tests?**

Your task will be to evaluate your *Controls* to see if they address the *Inherent Risks* you’ve identified to your program or processes. Once you’ve performed your preliminary assessment, the next step is to prepare test plans for those controls determined to have low control risk – that is, controls believed to be working as intended. Only low risk controls *must* be tested. Controls that are rated as having *High Risk* are assumed ineffective or non-existent, and corrective action plans should be developed to remediate the control weakness. Moderate risk controls may be tested and monitored by management to determine if modification of the control is required

**How do I test my controls once I’ve identified our and our risks and the controls that are supposed to mitigate their impact?**

Document what you plan to Test Controls on the *Test Plan Form* (**attachment 3**) to help you organize you planned tests. The instructions are included with the form. Not all elements of the form will apply to your evaluation. In order to evaluate if the proper *Controls* are in place, are effective, and being used you should test them. There are four ways to test *Controls*:

*Interviewing* is appropriate for many evaluations. (Surveys are a form of interview.) You should construct interview questions that go to the effectiveness and the implementation of controls and document them.

*Observing* is appropriate when a process is the control and produces no examinable product for inspection. Observation is appropriate when access to an area is restricted to authorized personnel only.

*Inspecting* is an appropriate test method when documentation is available to check for such controls as authorization, time schedules, or contract compliance.

*Reperformance* is most appropriate when testing information systems to ensure that expected output is a consequence of operational input. An example of reperformance is entering invalid data into a mandatory data field to see if they system performs a fatal edit.

Perform the tests using the test plan as prepared and report the results of the test on the *Test Plan Form* and on the *Control Assessment Form* (**both part of attachment 3**).

**So now I've conducted my test and have the results that I've documented the results in the excel workbook. What do I do next?**

Management must evaluate the results of control testing. As a result of the evaluation of the design and operating effectiveness of the controls, management will conclude whether:

- There are or are not control gaps;
- The design of the control is effective or not effective; and/or
- The operating effectiveness of the control is effective, partially effective or not effective.

Management should consider whether an ineffective control would create the potential for a high risk condition to occur, operations to be severely impacted, non-compliance conditions to exist, or financial reports to be misstated. Results will identify when a deficiency exists; judgment needs to be applied to decide whether the consequences of ineffective controls are significant enough to report as ***control deficiencies, reportable condition, or material weaknesses***.

A ***control deficiency*** exists when the testing of a control has failed.

A ***reportable condition*** is a control deficiency or combination of control deficiencies that are considered by management to be of significance and could adversely affect the program's ability to meet its mission.

A ***material weakness*** is a reportable condition that the Bureau/Office Director determines to be significant enough to be reported outside the agency and is included in the annual assurance statement and reported in the Bureau's/Office's AFR. Determining the level of deficiency requires a judgment by Bureau/Office managers as to the relative risk and significance of the deficiency.

Remember - Internal control reporting is subject to cost-benefit constraints, and no system is designed to provide **absolute assurance** that undesirable conditions will not occur. The Director signs an annual assurance statement that gives **reasonable assurance** that the Bureau has effective *Internal Controls*.

**Are there any other types of assessment for ICRs that can be performed?**

Internal Control Reviews are defined as any audit, review, evaluation, and inspection performed by internal individuals, groups, or teams originating in an organization that follows the steps and processes for the internal control cycle.

**Alternative Internal Control Review (AICR)** is defined as an evaluation of controls over activities of an assessable unit which have a potential for improving the effectiveness or efficiency of an operation. AICRs are conducted externally. Examples of

AICRs include inspections, evaluations, GAO and OIG audits, and OMB Circular A-133 Single Audits.

To consider whether internal reviews conducted by an organization support the Annual Assurance Statement qualify as AICRs, these reviews should:

- Be planned to consider the scope of the review to include the period covered and the extent of monitoring, testing, verification, and/or validation to be performed;
- Contain objectives or purposes of the review or report that align with and demonstrate compliance with Internal Control Program objectives;
- Identify the staff performing the review;
- Contain evidence that the review conducted demonstrates compliance with laws and regulations and/or that specific monitoring and testing was performed to determine compliance with the purpose/objectives of the review;
- Contain adequate documentation to support any conclusions drawn or deficiencies noted in a written format;
- Ensure deficiencies noted during an AICR are reported to the appropriate manager responsible for taking action to correct issues and must be reported to ensure that corrective action is tracked until implementation; and,
- Identify a person responsible for taking corrective action and a target date to address the deficiencies noted.

**External Reviews** are audits, reviews, or evaluations performed by an entity outside of the Bureau/Office. For the most part, these reports will originate with either the GAO or the Department's OIG. The reported results of these reviews may be used as support for the organization's Annual Assurance Statement.

Management may use other sources of information for planning purposes and to avoid duplication of conducting reviews. Sources of information may include:

- Management knowledge gained from daily operation of programs and systems (ICR);
- OIG and GAO reports, including audits, inspections, reviews, investigations or other products (AICR);
- Annual evaluation and reports pursuant to FISMA and OMB Circular A-130, *Management of Federal Information Resources*, or any other system reviews (ICR);
- Current year Program Assessment Rating Tool (PART) assessments (AICR); and,
- Single Audit reports for grant-making Bureaus/Offices (AICR).

However, the sources of information listed above should take into consideration whether the process included an evaluation of internal controls. Bureaus/Offices should avoid duplicating reviews that assess internal controls and should coordinate efforts with other evaluations to the extent possible.

Departmental Functional Reviews (DFR's) — To comply with statutory requirements and OMB directives, Interior's Offices of the Chief Information Officer (OCIO) and Acquisition and Property Management (PAM) will prescribe selected DFR's for IT systems, property, financial assistance (i.e., grants and cooperative agreements), acquisition management, and other functional areas deemed necessary. These DFRs should be treated as Internal Control Reviews (ICRs). Guidance for conducting and reporting the results of these reviews will be provided by the responsible offices.

**So I've completed my evaluation. How do I report this to WO-830?**

Your *Control Assessment form* has results reported in them. If *Internal Controls* are adequate then no further actions are required. If there is a *Material Weakness, Reportable Condition, or a Control Deficiency* a Corrective Action Plan (CAP) must be written (**attachment 4**) and submitted to WO-830 by the processes owners with the inadequate Controls.

**When is my final product due to WO-830?**

We need to have the results of your review not later than August 16, 2010. Additionally, you'll supply a copy of the Annual Assurance Statement for your Component signed by your AD at this time.

If you need any help contact Jacob Lee at 202-912-7080 or [Jacob\\_lee@blm.gov](mailto:Jacob_lee@blm.gov)