



USAID
FROM THE AMERICAN PEOPLE

The 2015 User Guide to the Uniform Risk and Internal Control Assessment Tool (URICA)

A Training Reference for ADS Chapter 596

Revision Date: 03/26/2015
Responsible Office: M/CFO/APC
File Name: TBD

Table of Contents

I. Internal Control Framework.....	3
A. USAID Internal Control Historical Background.....	3
B. Compliance with FMFIA.....	3
II. Important Dates.....	4
III. <i>GAO Standards for Internal Control in the Federal Government (Green Book)</i>	4
A. "The Cube" – Components of Internal Control.....	5
1. Control Environment Component.....	5
2. Risk Assessment Component.....	5
3. Control Activities Component.....	5
4. Information and Communications Component	6
5. Monitoring Component.....	6
B. "The Cube" – Objectives of Internal Control.....	6
1. Operations Objectives.....	6
2. Reporting Objectives.....	7
3. Compliance Objectives.....	7
C. "The Cube" – USAID Levels of Organizational Structure.....	7
D. "The Cube" – Documentation Requirements.....	7
IV. URICA (Uniform Risk and Internal Control Assessment).....	8
A. The URICA Process.....	8
1. Getting Started with URICA.....	9
2. Navigating URICA.....	10
3. Entering the Office (Column C).....	11
4. Identifying Risk or Concerns (Column D).....	12
5. Functional Areas (Column U), Business Process (Column V), and Risk Family (Column W).....	13
6. Likelihood of Risk (Column X), Magnitude of Impact (Column Y) and Risk Rating (Column Z)...	13
B. Determining a Risk Response Using Controls.....	14
1. Rating Controls Achieve Objectives (Column AD), Documented Internal Control Responsibilities (Column AE), and Documented Control Testing (Column AF).....	15
V. Evaluating and Finalizing the URICA Results.....	16
VI. Printing the Report.....	17
VII. URICA References.....	19
VIII. Annual FMFIA Certification.....	20

I. Internal Control Framework

A. USAID Internal Control Historical Background

In 1982, Congress enacted the *Federal Managers' Financial Integrity Act (FMFIA)*, 31 USC 3512, which requires each agency to establish and to maintain internal control systems that allow obligations and costs to be recorded in compliance with applicable laws; funds, property, and other assets to be safeguarded; and revenues and expenditures applicable to agency operations to be properly recorded and accounted for reliable financial information. Section II of FMFIA requires an assessment of *non-financial* controls to assure their effectiveness and efficiency and their compliance with laws and regulations. In September 2014, the Government Accountability Office (GAO) issued *Standards for Internal Control in the Federal Government (Green Book)* in order to provide a general framework for agencies to follow in designing their financial and non-financial internal control programs.

Although the *GAO Green Book* establishes the internal control standards for U.S. Agency for International Development (USAID), the Office of Management and Budget (OMB) has issued *OMB Circular A-123, Management's Responsibility for Internal Control*, to provide specific reporting guidance for USAID in implementing internal control programs. Each November, the USAID Administrator is required to transmit in the *Agency Financial Report (AFR)* a single annual Statement of Assurance to the President, Congress, and OMB, stating whether there is reasonable assurance that the USAID's internal controls are achieving intended objectives.

Both the *GAO Green Book* and *OMB Circular A-123* defines internal control as the steps USAID takes to provide reasonable assurance that USAID's objectives are achieved through: (1) Effective and efficient operations, (2) Reliable reporting, and (3) Compliance with applicable laws and regulations. The safeguarding of assets is a subset of all of these objectives. Internal controls are designed to provide reasonable assurance to prevent or detect unauthorized acquisition, use, and disposition of assets.

USAID has issued specific guidance in the *Automated Directives System (ADS) 596, Management's Responsibility for Internal Control*. The Office of the Chief Financial Officer; the Audit, Performance and Compliance Division (M/CFO/APC) is responsible for providing guidance and a specific methodology for implementing the Federal Managers' Financial Integrity Act (FMFIA) that reporting entities (Bureaus, Independent Offices and Missions) must follow to meet these requirements.

B. Compliance with FMFIA

USAID's management and employees are responsible for establishing and maintaining effective internal controls which include financial management systems that meet the objectives of FMFIA, the *Green Book*, and the revised *OMB Circular A-123*, which provides guidance for the execution of FMFIA. *ADS 596* provides the guidance for establishing an internal control program and annually evaluating internal controls and reporting on the status of any identified material weaknesses up through the chain of command to the President, Congress, and OMB. To support USAID reporting, all Bureaus, Independent Offices (B/IOs) and Missions are required to annually report on the status of their internal controls and the progress made in correcting prior reportable conditions.

In order to comply with the requirements of FMFIA and *OMB Circular A-123*, all departmental elements (inclusive of all integrated contractors) are required to perform one or more of the following types of internal controls assessments:

- Annual Certification Letter from all Missions and B/IOs;

- The Uniform Risk and Internal Control Assessment (URICA) Review; and
- Corrective Action Plans (CAPs) for any Material Weaknesses or Significant Deficiencies.

See the annual FMFIA Agency Notice detailing how internal control certification letters are to be completed.

II. Important Dates

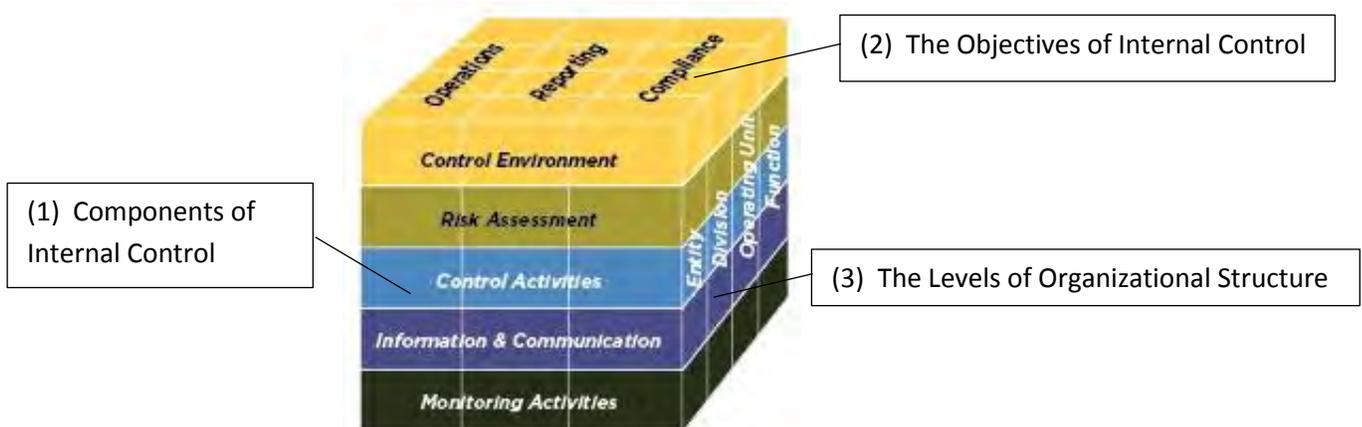
Each year an Agency Notice is published providing due dates for the annual FMFIA certification. The annual FMFIA requires submission of a certification letter, URICA review, and Corrective Action Plans (CAPs). If you have questions, check the Agency Notice for the M/CFO/APC points of contact.

III. GAO Standards for Internal Control within USAID

In 2014, GAO issued the latest *Standards for Internal Control in the Federal Government*, known as the *Green Book*. The *Green Book* outlines the standard USAID follows in establishing its internal control programs. The *Green Book* identifies five standards that “define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency’s operations: programmatic, financial, and compliance.”

Below is “The Cube” which models the *GAO Green Book* standards. “The Cube” consists of three dimensions: 1) The Components of Internal Control; 2) The Objectives of Internal Control; and 3) The Levels of Organizational Structure. By using “The Cube” shorthand below there are sixty or more possible cuboids (little cubes) or sets of combinations covering the GAO’s 17 Principles of Internal Control and 48 attributes (principles explained in detail), contained in the *Green Book*. Functions can be broken into multiple cuboids to express the business or operational processes. These cuboids address on various aspects (principles and attributes) of the internal control standards and allow one to focus and approach internal control deficiencies systematically.

$$Internal\ Control_{cuboid\ n} = \{(Component\ of\ IC), (Objective\ of\ IC), (Level\ of\ Organization)\}$$



A. “The Cube” – Components of Internal Control

1. Control Environment Component

The control environment consists of the Mission’s, B/IO’s organizational structure and culture created by management and sustained by employees that provides organizational support for effective internal control. The assessment should include obtaining a sufficient knowledge of the control environment to understand management’s attitude, awareness, and actions concerning the control environment. The assessment should consider the collective effect on the control environment, since management’s strengths and weaknesses can have a pervasive effect on internal control. Specific elements of the control environment that should be considered include:

- integrity and ethical standards;
- commitment to competence;
- management philosophy and operating style;
- organizational structure;
- assignment of authority and responsibility; and
- human resources policies and practices.

2. Risk Assessment Component

Risk assessment is the process by which management identifies internal and external risks that may prevent the USAID entity from meeting its mission objectives. The assessment should determine how management identifies risks, estimates the significance of risks, assesses the existence of risks in the current environment, and relates them to operations. The assessment should include obtaining sufficient knowledge of the agency’s process on how management considers risks relevant to mission objectives and decides about actions to address those risks. The results of this assessment at the USAID entity-level will drive the extent of testing and review performed of internal controls. Some significant circumstances or events that can affect risk include:

- complexity or magnitude of programs and operations;
- extent of manual processes or applications;
- changes in operating environment;
- new personnel or significant personnel changes;
new or revamped information systems;
- significant new or changed programs or operations;
- new technology; or
- new or amended laws or regulations.

3. Control Activities Component

Control activities are the mechanisms that help ensure that management directives are carried out, mission objectives are met, and risks are effectively mitigated. The assessment should include obtaining an understanding of the control activities applicable at the USAID entity-level, such as:

- policies and procedures;
- management objectives (clearly written and communicated throughout the agency);
- planning and reporting systems;
- analytical review and analysis;
- segregation of duties;

- safeguarding of assets; and
- physical and access controls.

4. Information and Communication Component

Relevant, reliable, and timely information should be communicated within the organization to relevant personnel at all levels and externally to outside stakeholders. The assessment should include obtaining an understanding of the information system(s) relevant to performance of mission objectives. Such an understanding should include:

- the type and sufficiency of reporting produced;
- the manner in which information systems development is managed;
- disaster recovery;
- communication of employees' control-related duties and responsibilities; and
- how incoming external communication is handled.

5. Monitoring Component

The effectiveness of internal controls should be monitored during the normal course of business. The URICA and FMFIA certification letter should include obtaining an understanding of the major types of activities the USAID entity-level uses to monitor internal controls, including the source of the information related to those activities and how those activities are used to initiate corrective actions. Required submissions include:

- FMFIA Certification letters from the B/IOs and Missions;
- The B/IO's and the Mission's URICA; and
- The B/IO's and the Mission's Corrective Action Plans (CAPs) for material weaknesses and significant deficiencies.

B. "The Cube" -- Objectives of Internal Control

Management groups objectives using, "The Cube," (See page 4) into one or more of the three categories of objectives:

- **Operations** - Effectiveness and efficiency of operations;
- **Reporting** - Reliability of reporting for internal and external use; and
- **Compliance** - Compliance with applicable laws and regulations.

Safeguarding of Assets -- A subset of "The Cube's" three categories of objectives is the safeguarding of assets. Management designs an internal control system to provide reasonable assurance regarding prevention or prompt detection and correction of unauthorized acquisition, use, or disposition of an entity's assets.

1. Operations Objectives

Operations objectives relate to program operations that achieve an entity's mission. An entity's mission may be defined in a strategic plan. Such plans set the goals and objectives for an entity along with the effective and efficient operations necessary to fulfill those objectives. Effective operations produce the intended results from operational processes, while efficient operations do so in a manner that minimizes the waste of resources. Management can set, from the objectives, related sub-objectives for units within the organizational structure. By linking objectives throughout the entity to the mission, management improves the effectiveness and efficiency of program operations in achieving the mission.

2. Reporting Objectives

Reporting objectives relate to the preparation of reports for use by the entity (B/IO or Mission), its stakeholders, or other external parties. Reporting objectives may be grouped further into the following subcategories:

- External financial reporting objectives - Objectives related to the release of the entities financial performance in accordance with professional standards, applicable laws and regulations, as well as expectations of stakeholders.
- External nonfinancial reporting objectives - Objectives related to the release of nonfinancial information in accordance with appropriate standards, applicable laws and regulations, as well as expectations of stakeholders.
- Internal financial reporting objectives and nonfinancial reporting objectives - Objectives related to gathering and communicating information needed by management to support decision making and evaluation of the entity's performance.

3. Compliance Objectives

At USAID, objectives related to compliance with applicable laws and regulations are very significant. Laws and regulations often prescribe an entity's (B/IO or Missions) objectives, structure, methods to achieve objectives, and reporting of performance relative to achieving objectives. Management considers objectives in the category of compliance comprehensively for the entity and determines what controls reporting objectives relate to the preparation of reports for use by the entity, its stakeholders, or other external parties.

C. "The Cube" – USAID Levels of Organization Structure

Management groups the organizational structure using, "The Cube," (See page 4) into one of four levels:

- **Entity** – B/IOs and Embassies (if co-located);
- **Division** – USAID Mission or B/IO division (USAID/W);
- **Operating Unit** – Mission office or B/IO branch (USAID/W); and
- **Function** – Many different operational, programmatic, business or business support processes.

"The Cube" applies to both large and small USAID entities. However, smaller USAID entities (small Missions or small B/IOs) may have different implementation approaches than larger USAID entities (large Missions or large B/IOs). Smaller USAID entities typically have unique advantages, which can contribute to an effective internal control system. These may include a higher level of involvement by management in operational processes and direct interaction with personnel. Smaller USAID entities may find informal staff meetings effective for communicating quality information, whereas larger entities may need more formal mechanisms—such as written reports, intranet portals, or periodic formal meetings—to communicate with the organization. A smaller USAID entity, however, faces greater challenges in segregating duties because of its concentration of responsibilities and authorities in the organizational structure. Management, however, can respond to this increased risk through the design of the internal control system, such as by adding additional levels of review for key operational processes, reviewing randomly selected transactions and their supporting documentation, taking periodic asset counts, or checking supervisor reconciliations.

D. "The Cube" – Documentation Requirements

Documentation is a necessary part of an effective internal control system. The level and nature of documentation vary based on the size of the USAID entity and the complexity of the operational processes the

USAID entity performs. Management uses judgment in determining the extent of documentation that is needed. Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system. The *Green Book* includes minimum documentation requirements as follows:

- If management determines that a [GAO Green Book] principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.
- Management develops and maintains documentation of its internal control system.
- Management documents in policies the internal control responsibilities of the organization.
- Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.
- Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.
- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.

These requirements represent the minimum level of documentation in an USAID entity's internal control system. Management exercises judgment in determining what additional documentation may be necessary for an effective internal control system. If management identifies deficiencies in achieving these documentation requirements, the effect of the identified deficiencies is considered as part of management's summary determination as to whether the related principle is designed, implemented, and operating effectively.

IV. URICA (Uniform Risk and Internal Control Assessment)

Accurate assessments of both financial and non-financial risks are integral to performing effective internal control evaluations integrating the *GAO Green Book* principles for an entity. The Office of the Chief Financial Officer, specifically, the Audit, Performance and Compliance (M/CFO/APC) developed the Uniform Risk and Internal Control Assessment (URICA) to identify risks and associated controls, to calculate a risk priority and internal control deficiency (Material Weakness, Significant Deficiency, Control Deficiency and Acceptable Control), and to allow management to decide the deficiency. URICA is an Excel spreadsheet pulling together internal control references and standardizing the risk assessment methodology used throughout USAID. URICA calculates a result (priority number) based upon user entries. The executive for the B/IO or Mission then decides the level of the deficiency classification. For example, a Mission identifies risk and control factors which calculate a significant deficiency. Mission management, upon review of other non-calculated factors decides to downgrade the URICA calculated deficiency to one of acceptable control.

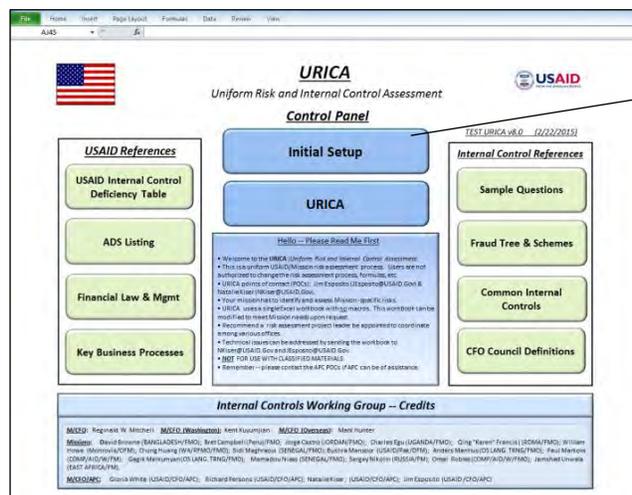
A. The URICA Process

Risks are assessed in a five-step process, which includes: (1) Risk identification, (2) Risk rating, (3) Control rating, (4) Deficiency prioritization and rating, and (5) Management's decision. URICA is a uniform process which should be performed at regular intervals and incorporated into existing processes, such as recurring program or project reviews. The user defines the risks, rates the risk, and identifies controls. URICA calculates the deficiency. Management decides if the calculated deficiency is correct.

1. Getting Started with URICA

Getting started with URICA requires the Internal Control Coordinator (ICC) from the Mission or Office to download URICA from the USAID M/CFO/APC Google site. See the Agency Notice regarding FMFIA. URICA is a spreadsheet requiring the user have basic Excel skills. This may require the ICC to work with various offices to establish basic Excel skills. The ICC will also have to plan how you will conduct the URICA review. For example, how will you distribute the spreadsheet file and training personnel in the various offices? How will you pull together the various office URICA inputs? Will you use one spreadsheet or multiple spreadsheets? The trade-off in using one spreadsheet is time for each office to complete the FMFIA process versus the ICC taking on the responsibility for consolidating the spreadsheet inputs from the various offices. The option of using Google *Sheets* is not available for the 2015 URICA process.

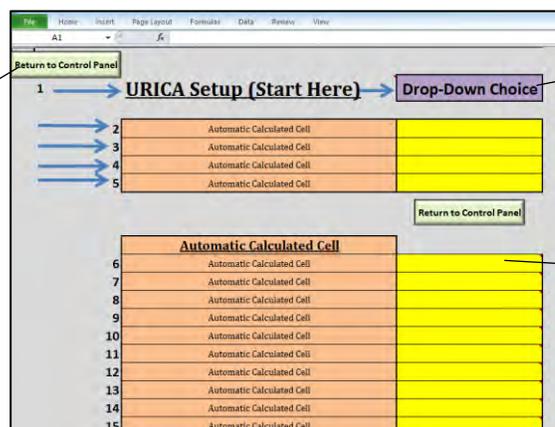
Open URICA as you would any Excel file. Once open, you should see the *Control Panel* screen.



(1) For the first-time ICC, start by selecting the *Initial Setup* button.

Should another screen appear, find the hyperlink on the panel and return to the *Control Panel* hyperlink. Once the *Control Panel* appears, you will note the green and blue buttons. The green buttons are internal control references. The blue buttons are the *URICA* and *Initial Setup* panels. The reference panels will be addressed later in this manual.

Start from the *Control Panel* by left-clicking on the *Initial Setup* button as shown above. On the Initial Setup screen, the ICC will have the ability to establish the various offices conducting the risk assessment.

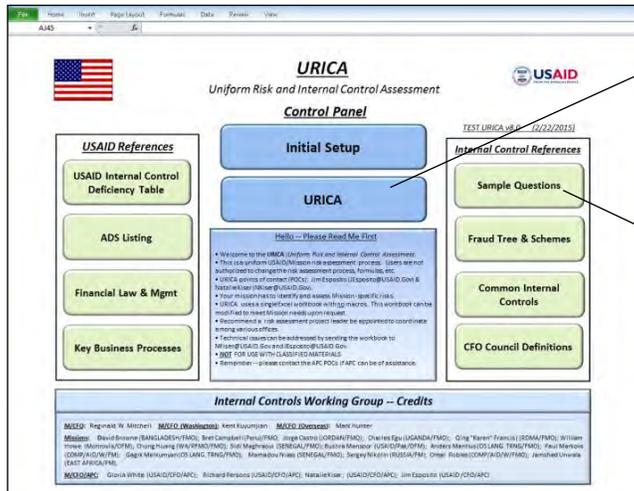


(2) This is a drop-down choice. Select the type of organization using URICA.

(4) When finished entering offices, left-click on this button to return to the *Control Panel*.

(3) Enter one office per yellow cell. There are 15 offices which can be entered into URICA.

Once the user has returned to the *Control Panel*, left-click on the *URICA* button to begin the review.



(5) Left-click on *URICA* to start the risks and controls assessment.

(Important Note) The user may refer to sample questions if desired. The questions can be copied and pasted into URICA.

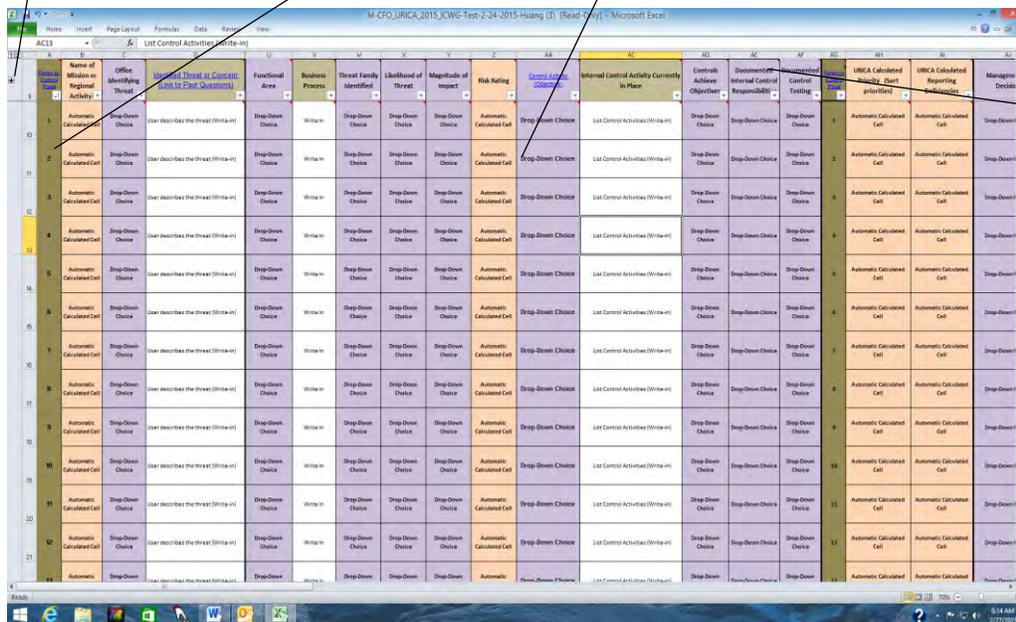
2. Navigating URICA

URICA navigation requires the user to have some basic familiarity with Excel such as drop-downs, groupings and filters. URICA uses a color coding and wording to aid the user. See the below.

(6) Grouping – left-clicking on this “+” icon opens the Heads-up Display. Once open, the icon changes to “-“. Left-clicking on “-“ closes the Heads-up display.

(7) Automatic calculated cells (tan cells) are formula cells. The user should tab over these cells.

(8) Drop-Down Choice cells (purple cells) require the user to click on the cell to get the drop-down choices.

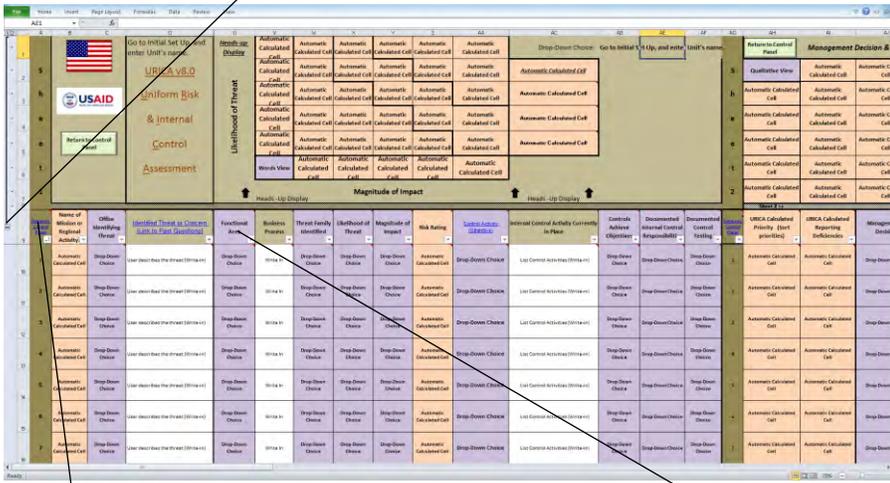


(9) All cells in Row 9 have user help tips.

(10) Row 9 has column filters. Left-clicking allows the user to select column filters or sort.



(11) Heads-up display is located from rows 1 through 8. Recommend keeping it closed when entering data. Once done, the user can open. This display is sensitive to user filter selections. The heads-up display is opened by selecting the row grouping to the left.



(12) Hyperlink to return to Main Control Panel.

(13) Freeze frame – Cell U10 is the freeze frame. The rows above row 9, unless the “Heads-Up Display,” is closed (it is open in the image above), and the columns (A through D) remain fixed as the user moves about the worksheet. Users entering data should return to column C (Office) of the next row to insure the you are in the proper frame.

3. Entering the Office (Column C)

URICA navigation requires the user to have some basic familiarity with Excel. URICA uses a color coding and wording to aid the user. Go to the column C (Drop-Down Choice). For the first user, this is row 9. Otherwise find a row where another user has not selected an office. Left-click on the cell and a drop-down selection of offices appears. If it does not, return to the Main Control Panel and select the Set-up button so you can enter offices.

(14) Hyperlink to Main Control Panel if user needs to return to the Initial Setup Screen.

(15) Select an office from the Drop-Down Choice.

Name of Mission or Regional Activity	Office Identifying Risks	Functional Area	Business Process	Risk Family Identified	Likelihood of Risk	Magnitude of Impact	Risk Rating	
1	Bureau APC	User describes the risk (Write-in)	Drop-Down Choice	Write In	Drop-Down Choice	Drop-Down Choice	Automatic Calculated Cell	
2	Automatic Calculated Cell	Drop-Down Choice	User describes the risk (Write-in)	Drop-Down Choice	Write In	Drop-Down Choice	Drop-Down Choice	Automatic Calculated Cell
3	Automatic Calculated Cell	Drop-Down Choice	User describes the risk (Write-in)	Drop-Down Choice	Write In	Drop-Down Choice	Drop-Down Choice	Automatic Calculated Cell
4	Automatic Calculated Cell	Drop-Down Choice	User describes the risk (Write-in)	Drop-Down Choice	Write In	Drop-Down Choice	Drop-Down Choice	Automatic Calculated Cell

4. Identifying Risk or Concerns (Column D)

What are the primary risks facing this office, Mission or B/IO? The user has the choice of creating their own questions or can refer to the Control Panel for sample questions used in previous years. The user should consider risks identified, but not limited to, one or more of the following: key business processes and sub-processes; cross-cutting functions, such as budgeting, human resources, information management, or contract management; or risks pertaining to specific organizational units. The following are examples using the, “If...then,” approach for identifying risks or concerns.

- Human Resources - *If* the program or office does not have a sufficient number of qualified staff and managers available to effectively manage, oversee, and close out its projects, *then* project or program objectives will not be met.
- Contractor Oversight - *If* the staff is unable to manage issues with contractor or awardee performance, such as performance or quality shortcomings, cost or schedule overruns, or non-compliance with laws and regulations, *then* waste, or abuse of government funds may occur and program objectives will not be met.
- Acquisition and Assistance - *If* a system is not in place to ensure competitiveness and fairness in contractor or awardee selection, *then* conflicts of interest may result.
- Budget Execution - *If* the organization does not follow established policies and procedures for budget execution, *then* government funds may be wasted, anti-deficiency violations may occur, and information regarding obligations, disbursements, and outlays may be inaccurate.
- Safeguards and Security - *If* security procedures are not fully documented, supported by training for the appropriate personnel, and followed, *then* non-compliance with security requirements could occur and USAID property could be damaged or employee safety could be at risk.

(16) Identified Risk or Concern – the user enters the concern in this column. The user can refer to past questions by left-clicking on the hyperlink in cell D9.

(17) The user has the option of using the 2014 URICA, the controller’s assessment, and Negropointe Memo questions.

5. Functional Areas (Column U), Business Process (Column V) and Risk Family (Column W) (Not Shown)

The Functional Areas requires the user to select the various general business processes. Once the user has completed this task, a specific business process can be identified in Column V. This allows all users to the ability to sort capability at a B/IO or Mission. Column W, not shown, allows the user to select a set of risk families. This provides another means of sorting and grouping various risks among up to 15 offices.

6. Likelihood of Risk (Column X), Magnitude of Impact (Column Y) and Risk Rating (Column Z)

In rating risks, the user selects from a drop-down list the likelihood of risk using words to describe the chance of the risk occurring. The magnitude of impact is if the risk occurs, what is the magnitude of the risk on the operating environment.

(18) Likelihood of Risk: The measure of the relative potential that the risk might occur given the operating environment.

(19) Magnitude of Impact: The estimate of the magnitude or nature of the effect that risk might cause given the operating environment.

(20) Risk Rating is expressed at low, medium or high risk.

D	U	V	W	X	Y	Z	AA
Identified Risk or Concern (Link to Past Questions)	Functional Area	Business Process	Risk Family Identified	Likelihood of Risk	Magnitude of Impact	Risk Rating	Control Activity (Objective)
If USDH hours are not promptly recorded in WebTA, there is the likelihood of fraud.	Audit and Internal Controls	WebTA	Fraud Risks	Unlikely	Minor	Low Risk	Drop-Down Choice
User describes the risk (Write-in)	Drop-Down Choice	Write In	Drop-Down Choice	Drop-Down Choice	Drop-Down Choice	Automatic Calculated Cell	Drop-Down Choice
User describes the risk (Write-in)	Drop-Down Choice	Write In	Drop-Down Choice	Drop-Down Choice	Drop-Down Choice	Automatic Calculated Cell	Drop-Down Choice

Initially, the likelihood and impact should be established assuming no controls are in place. This is referred to as the inherent or “exposure risk” rating. This is the URICA Calculated Priority (column AH).

X	Y	Z	AA	AC	AD	AE	AF	AG	AH	AI
Likelihood of Risk	Magnitude of Impact	Risk Rating	Control Activity (Objective)	Internal Control Activity Currently in Place	Controls Achieve Objectives	Documented Internal Control Responsibility	Documented Control Testing	Internal Control Eval	URICA Calculated Priority (Sort priorities)	URICA Calculated Reporting Deficiencies
Unlikely	Minor	Low Risk	Drop-Down Choice	List Control Activities (Write-in)	Drop-Down Choice	Drop-Down Choice	Drop-Down Choice	1	805	Material Weakness (URICA)

(21) URICA Calculated Priority – assumes no controls are in place. Once controls are rated the calculated priority usually decreases.

With the rating of controls (columns AA through AF), the risk and controls are again calculated again, with consideration to the control environment. The URICA Calculated Priority (Column AH) reflects the organization’s “real-life” operating environment. At a minimum, an annual FMFIA reassessment of risk ratings should be performed using URICA.

Ranking risk and controls helps to prioritize management’s attention to and decisions on the control environment. Risk rankings can be driven by measures of management concern (e.g., the dollars exposed; potential reputational damage; the anticipated cost to remediate an event, if the risk was to occur; the immediacy of the timeframe in which the risk could occur, etc.). In other words, if a risk were to impact near-term mission objectives, then management may prioritize that risk in its rankings.

When ranking risks, management should consider the URICA priority calculation in the context of these additional measures of concern. Those risks that management ranks highest are typically the risks that management will choose to mitigate first.

B. Determining a Risk Response Using Controls

After risks are assessed, management can then determine its risk response. Management should have a clear concept of its level of risk tolerance when determining what actions it will take to manage those risks that pose the greatest threat to achieving organizational objectives. For example, if management establishes a performance objective of 100%, is it willing to accept a result of 90%? Once its level of risk tolerance is set, management can choose its preferred risk response – to accept, avoid, reduce, share, or transfer a risk. In selecting its risk response, management should give consideration to the current operating environment, including what existing processes can be leveraged to manage certain risks.

Establishing controls to manage risk is a common risk response. Typically, controls are put into place when the choice is to reduce or share a risk. Controls also may be implemented to avoid a risk. Management should keep in mind that controls can provide only reasonable assurance – not absolute assurance – that the risks will be mitigated. The risk that remains, or residual risk, should be within levels acceptable to management.

1. Rating Controls Achieve Objectives (Column AD), Documented Internal Control Responsibilities (Column AE) and Documented Control Testing (Column AF)

The determination of the effectiveness of controls is driven by three major factors: (1) Controls achieving objectives; (2) Documented internal control responsibilities; and (3) Documented control testing.

(22) Rating controls – Achieving objectives; Documented internal control documentation; and Documented internal control testing.

D	W	X	Y	Z	AA	AC	AD	AE	AF	AG	AH	AI
Identified Risk or Concern (Link to Fast Questions)	Risk Family Identified	Likelihood of Risk	Magnitude of Impact	Risk Rating	Control Activity (Objective)	Internal Control Activity Currently in Place	Controls Achieve Objectives	Documented Internal Control Responsibilities	Documented Control Testing	Result to Control Eval	URICA Calculated Priority (Sort priorities)	URICA Calculated Reporting Deficiencies
If USDH hours are not promptly recorded in WebTA, there is the likelihood of fraud.	Fraud Risks	Unlikely	Minor	Low Risk	Accurate and Timely recording of Transactions	Tone from the top regarding accurate and timely recording of transactions; Periodic audits; and Controls over Information Processing	Possible	Low	Yearly Testing	1	213	Control Deficiency (URICA)

(23) URICA Calculated Priority – Notice with the controls being evaluated offsets the risk. The priority number dropped from 805 (Material Weakness) to 213 (Control Deficiency).

Control Achieves Objectives (Column AD): Controls should assess to ensure they are functioning properly and effectively to achieve objectives. Areas where risk is deemed highest may require a strengthening of existing controls or additional controls to be put in place. If, in the evaluation process, one finds that an area of high risk has insufficient controls to adequately mitigate the risk, management should consider redesigning the existing controls. Alternatively, management can consider implementing additional controls. When determining the need for additional controls in high risk areas, managers must balance the cost of implementing an additional control with the benefit that control will bring in terms of added risk mitigation. There will be some areas in the high risk category that are inherently risky. The placement of additional controls may not result in greater mitigation in such instances.

Documented Internal Control Responsibilities (Column AE): Documented internal control responsibilities requires documented processes consider the internal control activities currently established paying attention to the segregation of duties, fraud, management override and identification of areas where controls are ineffective or insufficient.

Documented Control Testing (Column AF): Controls that are documented should have documented control testing performed. Documented control testing should be performed on a periodic basis: quarterly, annually, biannually, triennially, or randomly. No control testing with poor control documentation requires action be taken by management to return the business process to acceptable control. Generally speaking, sound business practices dictate that not all controls are tested every year except in instances of previously reported significant deficiencies and material weaknesses. Risk assessments help to determine the frequency with which controls are tested. Controls in areas that have the highest risk should be tested more often than controls in areas that pose lower risk. In a three-year test cycle, for example, controls in high risk areas should be tested annually, while those in moderate risk areas are tested biannually and those in low risk areas are only tested once every three years. Previously reported significant deficiencies and material weaknesses should be tested each year until the controls are no longer deficient. The Agency’s internal control program team (ICPT) of M/CFO/APC is available to provide assistance.

There are a variety of different techniques available to test internal controls. Below are just a few that may be considered in conducting tests of internal controls.

- Interviews, which can be either in-person or through the use of questionnaires. In general, it is considered a best practice to have information gathered from interviews be corroborated with a secondary type of evidence. However, this may not always be possible.
- Direct observation of performance of the control.
- Physical examination or inspection of documents.
- Transaction testing and re-performance, the latter being most commonly used when testing automated controls.

Organizations may employ a variety of evaluation activities and consider a wide-range of reliable existing information to effectively test internal controls. Examples of typical activities and considerations that may be used include, but are not limited to:

- Management Priorities;
- Consideration of the results of Inspector General (IG) and GAO audit reports (required in all cases);
- Review of prior-year Assurance Statement submissions;
- Review and analysis of performance reporting results;
- Consideration of the results of other internal or external assessments;
- Conduct of management meetings or interviews with critical staff regarding key control areas;
- Review of relevant management reports (e.g., safety manager reports, infrastructure status reports, etc.); and
- Review and analysis of other relevant and reliable information.

URICA entries use dual-purpose testing. Dual-purpose testing is designed to evaluate both control execution (i.e., did the control operate as intended) and risk occurrence (i.e., is there evidence that the stated risk occurred). Dual-purpose testing is important because it provides a mechanism for ensuring that controls are actually effective in risk mitigation, thereby reinforcing the site's control design effectiveness decision. Evaluating risk and controls should clearly convey this type of dual-purpose testing, recognizing that in some cases control execution and risk occurrence are tested simultaneously.

V. Evaluating and Finalizing the Control Assessment Results

The URICA Calculated Priority (column AH) and URICA Calculated Reporting Deficiencies (column AI) should support management's judgment (column AJ) whether the internal controls given a risk are functioning adequately. Exceptions noted in the testing of properly designed internal controls could indicate ineffectiveness. Management must consider the extent of a deficiency in such cases.

Deficiencies can range from *acceptable control* to a *material weakness*. URICA calculated the deficiency based upon the priority number (column AH). The priority number is a relative number based upon the user inputs. Management should consider the USAID internal control deficiency table when making a final determination (column AI).

(24) Management’s Decision – Management decides if the control is acceptable based upon risk tolerance or if a deficiency is needed. The Internal Control deficiency table (found in URICA references) should be consulted.

(25) Automatically determines if a Corrective Action Plan (CAP) is needed.

AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM
Internal Control Activity Currently in Place	Controls Achieve Objectives	Documented Internal Control Responsibility	Documented Control Testing	Return to Control Flag	URICA Calculated Priority (Sort priorities)	URICA Calculated Reporting Deficiencies	Management’s Decision	Corrective Action Plan (CAP) Needed in CACS?	Management Decision Comments (if different from URICA Calculated Deficiencies)	Decision Executive
Tone from the top regarding accurate and timely recording of transactions; Periodic audits; and Controls over Information Processing	Possible	Low	Yearly Testing	1	213	Control Deficiency (URICA)	Acceptable Control (Mgmt Decision)	None	Controls are being documented and management has decided the controls are acceptable.	Tom Jones (Mission Director)

Regardless of the acceptable threshold established by management and the number of exceptions noted in testing internal controls, management needs to assess the exposure that **any** exception creates for the organization to determine the results. For example, with high-risk processes, with strong internal controls and exceptions may have a significant impact on the control environment.

(26) Finalizing the Row Evaluated – The remaining columns provide the user the ability to enter data such as POCs, CACS numbers and file locations.

AH	AI	AJ	AK	AL	AM	CF	CG	CH
URICA Calculated Priority (Sort priorities)	URICA Calculated Reporting Deficiencies	Management’s Decision	Corrective Action Plan (CAP) Needed in CACS?	Management Decision Comments (if different from URICA Calculated Deficiencies)	Decision Executive	Unit’s Point-of-Contact (POC)	CACS Folder Number for NEW CAPs Only	Specific File Locations of Risk Assessment Supporting Documentation
213	Control Deficiency (URICA)	Acceptable Control (Mgmt Decision)	None	Controls are being documented and management has decided the controls are acceptable.	Tom Jones (Mission Director)			

VI. Printing the Report

URICA is designed to print a report using legal paper (8.5” x 14”) or paper of similar size. Before printing the report, the user should consider using the filters located in row 9 to eliminate rows not used. For example, if the user has entered data in row 10, a filter could be applied using cell D9 to eliminate all column cells with the phrase, “User describes the risk (Write-in).” Eliminating the phrase will hide rows not containing data and shorten the printing.

Below is an image of the printed report. Note the, “Heads-Up Display,” is shown which provides useful users summary data. The data in the, “Heads-up Display.” This helps summarize for the user the descriptive measure of the URICA review. The report concatenates the columns A through D with the end columns of URICA.

VIII. Annual FMFIA Certification

USAID publishes an Agency Notice each year for the FMFIA exercise. The Agency Notice contains detailed information regarding the submission of the FMFIA Certification letter. The submission of the FMFIA Certification letter along with the URICA review is required to be completed in the Consolidated Audit and Compliance System (CACS).

Should assistance be required by Internal Control Coordinator (ICC) for the B/IO or Mission, please contact Natalie Kiser (NKiser@USAID.Gov) for URICA, or Teresa Frakes (TFrakes@USAID.Gov) for CACS. Jim Esposito (JEsposito@USAID.Gov) is the backup for each of these areas.

One final note – development of URICA was a USAID collaborative effort. With no funding, the internal control working group set out to eliminate the outdated checklist to provide the Agency a standard calculation taking an algebraic word problem and translating it to a semi-quantitative value, blending risks and controls, and prioritizing it. To this end, the working group achieved its goal. URICA requires the users commit to working with integrity to conduct a review of risks and internal controls. Organizations with the right, “Tone from the Top,” will identify and understand their organizations risks and develop the means to reduce these risks using controls. Internal controls need to be recognized as a part of our daily work, not an addition to it. With the ever growing complexity of the business process systems, management has the choice of implementing a realistic working system of documented and tested internal controls or await the inevitable surprise and chaos that will occur when neither documented nor tested internal controls exist. Users are encouraged and thanked in advance for providing their suggestions to continually improve URICA.