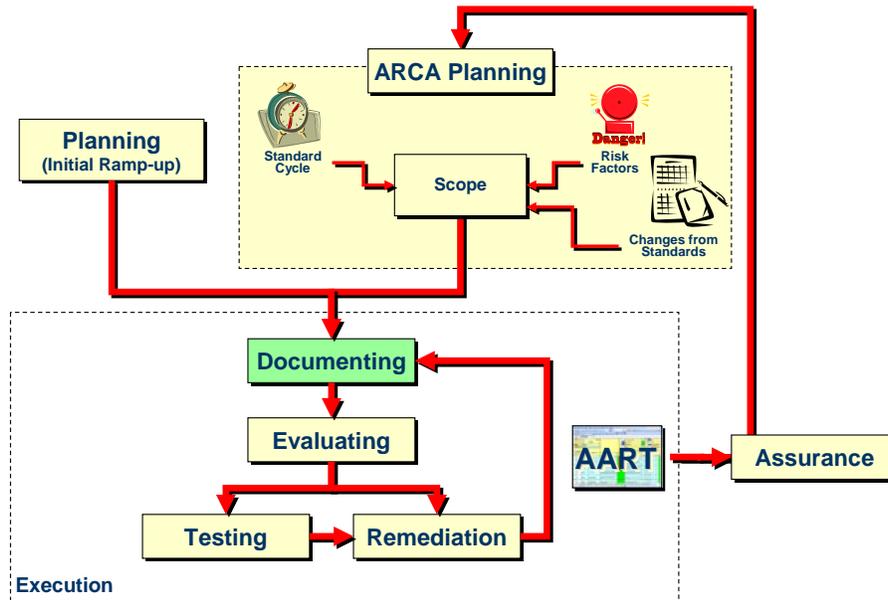




A-123 Quick Start Guide - Documenting



Purpose	<ul style="list-style-type: none"> Manage/develop documentation required for evaluating internal controls over financial reporting that will withstand the rigors of audit and record documentation attributes into the AART.
Key Activities	Identify and Record <ul style="list-style-type: none"> Entity Level Risks and Controls Processes and Sub-Processes Sub-Process Risks and Controls Financial Statement Assertions Location of Source and Detailed Documentation
Required Templates	<ul style="list-style-type: none"> AART Tool Suite Implementation Plan

<http://www.cfo.doe.gov/progliaison/doeA123/index.htm>

A-123Helpdesk@hq.doe.gov



A-123 Quick Start Guide – Documenting

Document Legend			
	Notebox: Contains additional information		Tip: Contains helpful information and recommendations.
	Requirements: Contains very important requirement information		Detailed A-123 Documentation
			AART Input: Color dependent by tab. Local AART [yellow], ECS-Assess [dark blue], PCS-Assess [light blue], ECS/PCS-Test [green], CAP-Track [red]

INTRO

ENTITY CONTROLS

Entity Controls relate to the **organization as a whole and are not specific to processes**. Good Entity Controls ensure the integrity and effectiveness of the organization and its leadership. Entity Control evaluations focus on 5 key management objectives¹: control environment, control activities, monitoring, risk assessment, and information and communication.



Entity controls cross cut all program activities (financial and non-financial). However, the A-123 evaluation focuses only on Entity Controls relevant to financial management areas that directly or indirectly impact financial reporting. As such, all of the Entity Controls (financial and operational) will need to be considered as they relate to and impact the following Financial Management Areas:

- Purchase card program management
- CO/COR roles and responsibilities
- Budget execution (carryover balances, prior year deobs., expired approps. mgmt, etc.)
- Financial management performance metrics
- Procurement (requisitions, purchase orders, etc.)
- Field/Site CFO liaison/operational awareness
- Proprietary/cuff systems
- Audit resolution and follow-up (financial related)
- Funds distribution
- Travel management/oversight
- Cost management (including accruals)
- Funds control

NOTE: This is not an exhaustive list of the financial management areas that could be impacted. Locations should independently evaluate what other financial management areas should be considered.

PROCESS CONTROLS

Good Process Controls ensure the **integrity and accuracy of the business transactions** as they impact the financial statements from a Presentation and disclosure; Existence and occurrence; Rights and obligations; Completeness and accuracy and Valuation or allocation (PERCV²) perspective.

In some cases, Process Controls may supplement Entity Controls to mitigate the same type of risk. An example of this is Segregation of Duties where proper procedures and policies are put in place and are supplemented by automated system controls at the process level.



A-123 Quick Start Guide – Documenting

 *Completing the AART Tool Suite is a requirement; however the data in the AART is summarized data and does not fulfill the complete A-123 Documentation requirements. Detailed A-123 Documentation and Source documentation³ should be maintained locally and be readily available in the event of an audit or other review.*

Entity Control Summary (ECS)

A. Identify and Record Entity Inherent Risk Statement⁴

- Review the standard ECS sub-categories and determine the inherent risk statements associated with each of these sub-categories. There may be multiple risk statements associated with each sub-category, at least one inherent risk statement must be entered for each sub-category. Consider among other things the following,

- What could go wrong?
[Behavior]
- What effect would it have
[Result]

[Example 1- Integrity and Ethical Values](#)
Area: Control Environment
Sub-Category: Integrity and Ethical Values
Risk Statement: Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.

[Example 2 – Segregation of Duties⁵](#)

 A well formulated risk statement would include a clear definition of **behavior** and/or action and the **negative result** if this behavior and/or action should occur.

-  Record your risk statements in the ECS-Assess tab of the AART Tool Suite in the row associated with the appropriate Area and Sub-Category:

AART: ECS Assess VERSION 4.0				
Select View:				
FO	CH			
Attester	Ard Geller			
Implementer	Shelley Hart			
Date Updated	October 31, 2006			
<input type="button" value="Insert Row"/>		<input type="button" value="Delete Row"/>		
Ref Col	Cycle	Area	Sub-Category	Risks
	EC	Control Environment	Integrity and Ethical Values	Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.
	EC	Control Activities	Segregation of Duties	An employee who creates a requisition also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and / or abuse of

If you have more than one inherent risk statement per sub-category, select the sub-category then insert additional rows by clicking the "insert row" button. If you need to delete an additional row click the "delete row" button on the ECS-Assess tab.



A-123 Quick Start Guide – Documenting

3. Repeat these steps for all 31 sub-categories.

B. Assign the Inherent Risk Rating⁶ (Likelihood and Impact)



Inherent Risk considers the General Environment in which you operate; it **does not** consider any mitigating controls. General Environment would include things such as:

- Number of transactions
- Organizational structure
- Liquidity of assets
- Skill/knowledge of staff
- Value of transactions
- Span of control
- Political sensitivities
- Susceptibility to fraud and irregularity

1. **LIKELIHOOD** - Determine the likelihood of the inherent risk specified by the risk statement occurring. Likelihood is a measure of the relative potential that the inherent risk might occur given the general environment⁷. In determining Likelihood, consider among other things the following,

- a. Organizational Culture
 - i) Stability and focus of leadership
 - ii) Vision imparted by leadership to the organization
 - iii) Variety of backgrounds/knowledge of personnel
 - iv) Stability of workforce
 - v) Skill level and technical competence of workforce
- b. Type of organization
 - i) Co-location
 - ii) Size of distributed offices
 - iii) Size of business units
- c. Technological maturity
 - i) Level of integration

Example 1 – Integrity and Ethical Values

Area: Control Environment

Sub-Category: Integrity and Ethical Values

Risk Statement: Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.

Risk Likelihood: LOW - An organization of 20 people co-located in a war room type of environment with strong, visible leadership.

Example 2 – Segregation of Duties⁸

2. **IMPACT** - Determine the relative magnitude of the impact if the inherent risk specified by the risk statement occurs. Impact is a measure of the magnitude/severity of the effect the risk's occurrence might cause given the general environment, considering both the nature and extent of the effect of the risk's occurrence. In determining Impact, consider among other things the following:

- a. Span of Control (breadth of organizations impacted)
- b. Potential Liability due to type of business

Example 1 – Integrity and Ethical Values

Area: Control Environment

Sub-Category: Integrity and Ethical Values

Risk Statement: Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.

Risk Likelihood: LOW - An organization of 20 people co-located in a war room type of environment with strong, visible leadership.

Risk Impact: HIGH - Business units responsible for the management of the nuclear material stockpile (high financial liabilities).

Example 2 – Segregation of Duties²



A-123 Quick Start Guide – Documenting

- Record the Likelihood and Impact Ratings for the associated inherent risk specified by the risk statements in the ECS-Assess tab of your AART Tool Suite:

AART: ECS Assess VERSION 4.0							
Select View:							
FO	CH						
Attester	Ard Geller						
Implementer	Shelley Hart						
Date Updated	October 31, 2006						
<input type="button" value="Insert Row"/> <input type="button" value="Delete Row"/>							
Ref Col	Cycle	Area	Sub-Category	Risks	Likelihood	Impact	Risk Assessment
	EC	Control Environment	Integrity and Ethical Values	Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices	L	H	H
	EC	Control Activities	Segregation of Duties	An employee who creates a requisition also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and / or abuse of government funds.	L	H	H

The overall Inherent Risk Assessment Rating will be automatically calculated for each risk statement based on the following rules:

Likelihood	+	Impact	=	Inherent Risk Assessment
Low		Low		Low
Low		Moderate		Low
Low		High		High
Moderate		Low		Low
Moderate		Moderate		Moderate
Moderate		High		High
High		Low		Moderate
High		Moderate		High
High		High		High

- It is highly recommended to document the general approach to performing your inherent risk assessment, including general environment considerations, likelihood and impact considerations, etc.



A-123 Quick Start Guide – Documenting

C. Identify and Record Key Entity Controls¹⁰

1. Collect all existing documentation related to the specified Entity risk statements and standard Sub-Categories, for example:
 - a. Code of Ethics
 - b. Policies & Procedures (Conflict of Interest Policies)
 - c. Organizational Structure Diagrams
 - d. HR Handbooks
 - e. IT controls (e.g. Security Profiles, Disaster Recovery Procedures)
2. Using source documentation, identify the existing controls that mitigate each inherent risk specified by the risk statement. To further identify the key controls, consider among other things the following:

- a. Priority and criticality of the control in mitigating the risk (key controls)
- b. Control Mode: Preventive[P] and Detective[D]¹¹
- c. Level of Automation (i.e. Manual, Partially Automated or Automated)
- d. Single Control or Multiple Controls (Control Set) can mitigate a specific risk

Example 1 – Integrity and Ethical Values

Area: Control Environment

Sub-Category: Integrity and Ethical Values

Risk Statement: Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.

Risk Likelihood: LOW - An organization of 20 people co-located in a war room type of environment with strong, visible leadership.

Risk Impact: HIGH - Business units responsible for the management of the nuclear material stockpile (high financial liabilities).

Control Objective: To promote and enforce ethical behavior:

Control Set: (1) Management has posted their integrity and ethical ideals in a guidance document entitled "Code of Conduct" on their website and in hard copies, and is distributed to all employees. [P] (2) All employees on every level must read, accept, and sign a document indicating they understand and will follow the guidance as outlined in the "Code of Conduct". [P] (3) Meetings are conducted that include integrity and ethical values as an agenda item and employees are required to attend once a year. [P] (4) Annual employee appraisals include a section to discuss employees' behavior. [D] (5) Management maintains an open door policy to ensure that any unethical behavior is reported and management looks into any reports. [D] (6) Management encourages anonymous e-mails to report unethical behavior. [D] (7) Management takes appropriate action immediately once an allegation of unethical or illegal behavior has been proven. [D] (8) Management has a "no-tolerance" policy and terminates anyone who commits unethical or illegal indiscretions. [D]

Example 2 – Segregation of Duties¹²



A-123 Quick Start Guide – Documenting

3. Record the key controls in the AART as a control set in the AART ECS-Assess tab in a single cell in the row associated with the related risk statement. Together, these controls represent the control set.

AART: ECS Assess							Overall Entity Control Ratings	
Select View:								
FO	CH							
Attester	Ard Geller						y Control Environment	
Implementer	Shelley Hart						y Control Activities	
Date Updated	October 31, 2006						y Information and Communication	
							y Risk Assessment	
							y Monitoring	
Ref Col	Cycle	Area	Sub-Category	Risks	Likelihood	Impact	R Assessment	
	EC	Control Environment	Integrity and Ethical Values	Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.	L	H		To promote and enforce ethical behavior: <ul style="list-style-type: none"> • Management has posted their integrity and ethical ideals in a guidance document entitled "Code of Conduct" on their website and in hard copies, and is distributed to all employees. [P] • All employees on every level must read, accept, and sign a document indicating they understand and will follow the guidance as outlined in the "Code of Conduct". [P] • Meetings are conducted that include integrity and ethical values as an agenda item and employees are required to attend once a year. [P] • Annual employee appraisals include a section to discuss employees' behavior. [D] • Management maintains an open door policy to ensure that any unethical behavior is reported and management looks into any reports. [D] • Management encourages anonymous e-mails to report unethical behavior. [D] • Management takes appropriate action immediately once an allegation of unethical or illegal behavior has been proven. [D] • Management has a "no-tolerance" policy and terminates anyone who commits unethical or illegal indiscretions. [D]

All key controls to offset a specific risk statement (i.e. the control set) MUST be recorded only in a single cell in the row corresponding to the risk statement.

D. Identify and Record Control Set Attributes

1. Determine the Control Set Mode of the key controls contained in each control Set: Preventive (P), Detective (D), or Both (P&D)¹³.
2. Determine if the Control Set is Entirely Automated (Aut), Entirely Manual (Man), or Partially Automated (Pau).
3. Determine the Control Set Frequency at which each control set is executed. In the case where controls within the control set are executed at different intervals (some monthly, some daily, etc), the frequency of the most critical key control should be indicated.

Control Set Frequency Options:

A = Annually **M** = Monthly **W** = Weekly **R** = Recurring*
Q = Quarterly **B** = Biweekly **D** = Daily

*Recurring frequency is a control that executes every time an activity or transaction is run. This may be numerous times in one day.



A-123 Quick Start Guide – Documenting



- Using the drop down boxes, record the appropriate values for the attributes of the specified control sets.

AART: ECS Assess										Overall Entity Control Ratings		
Select View:										Control Environment		
FO: CH										Control Activities		
Attester: Ard Geller										Information and Communication		
Implementer: Shelley Hart										Risk Assessment		
Date Updated: October 31, 2006										Monitoring		
Insert Row Delete Row												
Ref Col	Cycle	Area	Sub-Category	Risks	Likelihood	Impact	Risk Assessment	Controls	Prev/Det	Ctrl Type	Ctrl Freq	
EC		Control Environment	Integrity and Ethical Values	Management does not communicate, provide guidance, or practice its ethical values and/or standards to employees, suppliers, creditors, investors, customers, or other relevant parties resulting in unethical behavior and illegal practices.	L	H	H	To promote and enforce ethical behavior: <ul style="list-style-type: none"> Management has posted their integrity and ethical ideals in a guidance document entitled "Code of Conduct" on their website and in hard copies, and distributed to all employees. [P] All employees on every level must read, accept and sign a document indicating they understand and will follow the guidance as outlined in the "Code of Conduct". [P] Meetings are conducted that include integrity and ethical values as an agenda item and employees are required to attend once a year. [P] Annual employee appraisals include a section to discuss employees' behavior. [D] Management maintains an open door policy to ensure that any unethical behavior is reported and management looks into any reports. [D] Management encourages anonymous e-mails to report unethical behavior. [D] Management takes appropriate action immediately once an allegation of unethical or illegal behavior has been proven. [D] Management has a "no-tolerance" policy and terminates anyone who commits unethical or illegal infractions. [P] 	P&D	Man	M	
EC		Control Environment	Management's Commitment to Competence									
EC		Control Activities	Segregation of Duties	An employee who creates a requisition also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and/or abuse of government funds.	L	H	H	To prevent fraud, waste and/or abuse: <ul style="list-style-type: none"> Security rules are set up such that no single user can be assigned the roles of creating a requisition approving that requisition, approving a requisition creating the corresponding obligation, and creating the obligation and paying the invoice. [P] Workflow technology is implemented to automate work flow message distribution to monitor expenditures and approvals. [P] Workflow technology is implemented to enforce limits of authority management. [P] Only 3 Administrators have the authorization to create and/or change security profiles and work rules. [P] 	P&D	Aut	R	

E. [Highly Recommended] Record Location of Source and Detailed A-123 Documentation¹⁴

- In accordance with local documentation management policies, identify the location where the Source Documentation and the Detailed A-123 Documentation are maintained. Consider the following examples,

- Reference to available corporate policy
- Hardcopy version stored in a specific location
- Softcopy version stored on a shared drive
- Softcopy version stored on a website

Documentation Location Examples:
 Corporate Code of Ethics [Available on organization website]
 HR Recruiting Policy in HR Dept
 H:\DOE\HQ\Policies [Shared Local Drive]
 IT Department/System Security Handbook
 H:\DOE\HQ\A-123 Detail Docs\Risk Assessment Rationale [Shared Local Drive]



A-123 Quick Start Guide – Documenting

3. If source documentation does not exist or is incomplete, ensure the development of required documentation.

G. Identify and Record Sub-Processes

1. In the PCS Assess tab the processes annotated with a “Y” represent those that are related to your material accounts and require further evaluation.
2. For those relevant processes, use your existing source documentation to identify the sub-processes, and associate them with the standard DOE processes identified in the AART.



3. Using the drop down list, select the standard processes and enter your relevant sub-processes into the PCS-Assess tab (you must repeat the process selection for each sub-process entered).

AART: PCS Assess											
Select View:								BPC			
FO	CH							General Ledger Management			
Attester	Ard Geller							Funds Management			
Implementer	Shelley Hart							FBWT			
Date Updated	October 31, 2006							Cost Management			
								Insurance			
								Grants			
								Loans			
								P2P			
								y Acquisition			
								y Inventory Management			
								y Payable Management			
<input type="button" value="Insert Row"/> <input type="button" value="Delete Row"/>											
Ref Col	Process Cycle	Processes	Sub-Processes	Risks	Likelihood	Impact	Risk Assessment	Controls			
	P2P	Acquisition	Create Requisition								
	P2P	Inventory Management	Receive Goods & Services								
	P2P	Payable Management	Payee Information Maintenance								
	P2P	Payable Management	Disbursing								
	P2P	Payable Management	Invoice								



A-123 Quick Start Guide – Documenting

H. Identify and Record Inherent Risk Statements

1. Using the source documentation, identify all inherent risks at the activity¹⁵ level related to the sub-process. Consider key financial statement assertions (PERCV¹⁶) to validate the completeness of the identified risk statement.
 - a. What could go wrong in the Presentation and disclosure of financial information in the financial statements? [Behavior] and How significant could it be? [Impact]
 - b. What could go wrong in the Existence or occurrence of financial information in the financial statements? [Behavior] How significant could it be? [Impact]
 - c. What could go wrong in the Rights and obligations of financial information in the financial statements? [Behavior] How significant could it be? [Impact]
 - d. What could go wrong in the Completeness and accuracy of financial information in the financial statements? [Behavior] How significant could it be? [Impact]
 - e. What could go wrong in the Valuation or allocation of financial information in the financial statements? [Behavior] How significant could it be? [Impact]

[P] "Is it recorded in the right place?"

[E] "Did it happen and when?"

[R] "Do we own or owe what we think we do?"

[C] "Is anything missing?"

[V] "Are the numbers right?"

Example 1 – Disbursing

Process: Payable Management

Sub-Process: Disbursing

Risk Statement 1: Payments may be made in excess of approved contract amounts, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk Statement 2: Duplicate payments may be made for a single invoice, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Example 2 – Invoice¹⁷



A well formulated risk statement would include a clear definition of **fraudulent, wasteful and/or erroneous activities** and the **negative result** if these activities were to occur.



A-123 Quick Start Guide – Documenting

- Record your risk statements in the AART PCS-Assess tab in the row associated with the appropriate Process and Sub-Process: **(NOTE: There must be at least one risk statement for each sub-process)**

AART: PCS Assess				VERSION 4.0
Select View:				
FO	CH			
Attester	Ard Geller			
Implementer	Shelley Hart			
Date Updated	October 31, 2006			
<input type="button" value="Insert Row"/> <input type="button" value="Delete Row"/>				
Ref Col	Process Cycle	Processes	Sub-Processes	
	P2P	Payable Management	Disbursing	Invoice amount exceeds obligation and approved funding, resulting in non-compliance with the Anti-Deficiency Act.
	P2P	Payable Management	Disbursing	Duplicate payments may be made, resulting in extraordinary burden to the government due to potential loss of unrecoverable funds.

If you have more than one inherent risk statement per sub-process, select the sub-process then insert additional rows by clicking the "insert row" button. If you need to delete an additional row click the "delete row" button on the PCS-Assess tab.

- Record all of the financial statement assertions that are applicable to the inherent risk statement. Insert a "y" in the appropriate P,E,R,C, or V column.

AART: PCS Assess				VERSION 4.0										
Select View:														
FO	CH													
Attester	Ard Geller													
Implementer	Shelley Hart													
Date Updated	October 31, 2006													
<input type="button" value="Insert Row"/> <input type="button" value="Delete Row"/>														
Ref Col	Process Cycle	Processes	Sub-Processes	Risks	Likelihood	Impact	Risk Assessment	Controls	P	E	R	C	V	
	P2P	Payable Management	Disbursing	Invoice amount exceeds obligation and approved funding, resulting in non-compliance with the Anti-Deficiency Act.						Y	Y	Y	Y	
	P2P	Payable Management	Disbursing	Duplicate payments may be made, resulting in extraordinary burden to the government due to potential loss of unrecoverable funds.						Y	Y	Y	Y	
	P2P	Payable Management	Invoice	Invoice is approved for payment without receipt of goods and / or services, resulting in loss of funds to government and potential non-compliance with the Anti-Deficiency Act.						Y	Y	Y	Y	



A-123 Quick Start Guide – Documenting

I. Assign the Inherent Risk Rating (Likelihood and Impact)



Inherent Risk considers the General Environment in which you operate; it **does not** consider any mitigating controls. General Environment would include things such as:

- Number of transactions
- Organizational structure
- Liquidity of assets
- Skill/knowledge of staff
- Value of transactions
- Span of control
- Political sensitivities
- Susceptibility to fraud and irregularity

1. Determine the likelihood of the inherent risk statement occurring. Likelihood is the relative potential that the risk will occur in the General environment. In determining likelihood, consider among other things the following:

- a. Number of transactions
- b. Number of people with access
- c. Liquidity of assets or inherent susceptibility to theft or misuse

Example 1 – Disbursing

Process: Payable Management

Sub-Process: Disbursing

Risk Statement 1: Payments may be made in excess of approved contract amounts, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk 1 Likelihood: LOW - Payments relate to a small business unit with few, non-complex contracts.

Risk Statement 2: Duplicate payments may be made for a single invoice, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk 2 Likelihood: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month.

Example 2 – Invoice¹⁸



A-123 Quick Start Guide – Documenting

- Determine the relative magnitude of the risk impact if the inherent risk specified by the risk statement should occur. Impact is a measure of the magnitude/severity of the effect the risk might cause. In determining the Impact, consider among other things the following:

- Value of individual transactions
- Non-Compliance with laws and regulations
- Legal ramifications
- Public Relations impacts

Example 1 – Disbursing

Process: Payable Management

Sub-Process: Disbursing

Risk Statement 1: Payments may be made in excess of approved contract amounts, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk 1 Likelihood: LOW - Payments relate to a small business unit with few, non-complex contracts.

Risk 1 Impact: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month.

Risk Statement 2: Duplicate payments may be made for a single invoice, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk 2 Likelihood: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month.

Risk 2 Impact: LOW - Total value of all payment transactions is less than 0.5% of total operating budget.

E

Example 2 – Invoice¹⁹



- Record the Likelihood and Impact ratings in the PCS-Assess tab of the AART Tool Suite for the occurrence of the associated inherent risk, specified by the risk statement.

AART: PCS Assess					VERSION 4.0		
Select View:					B2C		
FO	CH						
Attester	Ard Geller						
Implementer	Shelley Hart						
Date Updated	October 31, 2006						
<input type="button" value="Insert Row"/> <input type="button" value="Delete Row"/>					P2P		
					y		
					y		
					y		
Ref Col	Process Cycle	Processes	Sub-Processes	Risks	Likelihood	Impact	Risk Assessment
	P2P	Payable Management	Disbursing	Invoice amount exceeds obligation and approved funding, resulting in non-compliance with the Anti-Deficiency Act.	L	H	H
	P2P	Payable Management	Disbursing	Duplicate payments may be made, resulting in extraordinary burden to the government due to potential loss of unrecoverable funds.	L	M	L
	P2P	Payable Management	Disbursing	Invoice is approved for payment without receipt of goods and / or services, resulting in loss of funds to government and potential non-compliance with the Anti-Deficiency Act.	L	L	L



A-123 Quick Start Guide – Documenting

4. It is highly recommended to document the general approach to performing your inherent risk assessment, including general environment considerations, likelihood and impact considerations, etc.
5. Repeat steps from Section G for all risk statements.

J. Identify and Record Key Process Controls²⁰

1. Using source documentation, identify the existing controls that mitigate each risk statement.

To further identify the key controls (which collectively represent a control set) consider, among other things, the following:

- a. Priority and criticality of the control in mitigating the risk (key controls)
- b. Control Mode: Preventive[P] and Detective[D]²¹
- c. Level of Automation (i.e. Manual, Partially Automated or Automated)
- d. Single Control or Multiple Controls (Control Set) can mitigate a specific risk

Example 1 - Disbursing

Process: Payable Management

Sub-Process: Disbursing

Risk Statement 1: Payments may be made in excess of approved contract amounts, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk 1 Likelihood: LOW - Payments relate to a small business unit with few, non-complex contracts.

Risk 1 Impact: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month.

Control Objective: To comply with Anti-Deficiency Act

Control Set: (1) System automatically closes contracts when receipts and invoices have been posted and paid equal to the amount of the contract.[P/Aut] (2) Invoices in excess of contract are automatically rejected with the reason code indicating that the contract is complete. [P/Aut] (3) Rejected invoices are sent back to appropriate departments for follow-up.[D/Pau]

Risk Statement 2: Duplicate payments may be made for a single invoice, resulting in loss to the Government (if not detected) and an increase in improper payment percentages reported to OMB (if later detected).

Risk 2 Likelihood: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month.

Risk 2 Impact: LOW - Total value of all payment transactions is less than 0.5% of total operating budget.

Control Objective: To prevent loss of funds.

Control Set: (1) System rejects entry of duplicate invoice numbers.[P/Aut] (2) System issues a warning if invoice numbers are different and amounts and payee are the same.[P/Pau] (3) Monthly report of potentially duplicate invoices is generated and reviewed by AP Supervisor.[D/Pau]

Example 2 – Invoice²²



A-123 Quick Start Guide – Documenting



- Record the key controls in the PCS-Assess tab in a single cell in the row associated with the related risk statement. Together, these controls represent the control set:

AART: PCS Assess					BCC			General Ledger Management
Select View:								Funds Management
FO	CH							FBWT
Attester	Ard Geller							Cost Management
Implementer	Shelley Hart							Insurance
Date Updated	October 31, 2008							Grants
								Loans
					P2P			Acquisition
								Inventory Management
								Payable Management
Ref Col	Process Cycle	Processes	Sub-Processes	Risks	Likelihood	Impact	Risk Assessment	Controls
	P2P	Payable Management	Disbursing	Invoice amount exceeds obligation and approved funding, resulting in non-compliance with the Anti-Deficiency Act.	L	H	H	To ensure that payments do not exceed approved funding: <ul style="list-style-type: none"> An invoice posted to an obligation in excess of approved, funded amount, is automatically placed on hold with appropriate reason code. (P) An e-mail is generated and sent to the appropriate parties. (P) A follow up report listing these invoices is sent to Budget, Procurement and A/P Managers. (P) If the hold is overridden, and an invoice is paid regardless of these controls, an additional set of e-mails and reports is generated and sent to Budget, Procurement and A/P Managers. (D)
	P2P	Payable Management	Disbursing	Duplicate payments may be made, resulting in extraordinary burden to the government due to potential loss of unrecoverable funds.	L	M	L	To eliminate duplicate payments: <ul style="list-style-type: none"> An invoice is entered and the number already exists, it is automatically rejected. (P) An invoice is entered and the number is different, but the obligation is fully depleted, the three-way matching functionality will automatically cause the invoice to be placed on hold with the reason code that the invoice is in excess of the contract / received quantities and / or amounts. (P) The duplicate invoice cannot be manually released for payment without changes in the contract and/or receipts to support the invoice. (P) An e-mail is generated and sent to responsible party advising of discrepancy. (P) A report is generated listing all invoices that are on hold with reason codes and is reviewed by the Accounting Manager weekly. (D)

All key controls to offset a specific risk (i.e. the control set) MUST be recorded in a single cell on the row corresponding to the risk statement.

K. Identify and Record Control Set Attributes

- Determine the Mode of the Control Set based on of the key controls contained in each control Set: Preventive (P), Detective (D), or Both (P&D).
- Determine if the Control Set is Entirely Automated (Aut), Entirely Manual (Man), or Partially Automated (Pau).
- Determine the Control Frequency at which each control set is executed. In the case where controls within the control set are executed at different intervals (some monthly, some daily, etc), the frequency of the most critical key control should be indicated.

Control Frequency Options:

A = Annually **M** = Monthly **W** = Weekly **R** = Recurring*
Q = Quarterly **B** = Biweekly **D** = Daily

*Recurring frequency is a control that executes every time an activity or transaction is run. This may be numerous times in one day.



A-123 Quick Start Guide – Documenting

M. Update the Implementation Plan

1.  Capture the status and barriers as well as any significant deviations encountered during the documenting phase.



A-123 Quick Start Guide – Documenting

SUPPLEMENTARY INFORMATION AND DEFINITIONS

¹ Key questions that should be considered for ECS:

- Has the management established and maintained an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management? (Control Environment)
- Has management initiated internal control activities to help ensure that their directives are carried out and are effective and efficient in accomplishing the agency's control objectives? (Control Activities)
- Has management established internal control monitoring that assesses the quality of performance over time and ensures that the findings of audits and other reviews are promptly resolved? (Monitoring)
- Has management assessed the risks the agency faces from both external and internal sources? (Risk Assessment)
- Has management communicated the importance of timely and appropriate information and communication throughout the organization to ensure that internal control and other responsibilities can be carried out effectively? (Information and Communication)

² As defined in the GAO/PCIE FAM Financial Statement assertions are Management's representations that are embodied in the account balance, transaction class, and disclosure components of the financial statements. The primary assertions are:

- Presentation and disclosure – the particular components of the financial statements are properly classified described and disclosed.
- Existence or occurrence – an entity's assets or liabilities exist at a given date and recorded transactions have occurred during a given period.
- Rights and obligations – assets are the rights of the entity and liabilities are the obligations of the entity at a given date.
- Completeness and accuracy – all transactions and accounts that should be presented in the financial statements are so included
- Valuation or allocation – asset, liability, revenue and expense components have been included in the financial statements at appropriate amounts.

³ The Source Documentation refers to materials that: Process - outline the specific processes and related process controls to be evaluated, Entity - that identify or support/represent the specific entity controls to be evaluated. The Detailed A-123 Documentation includes materials required to be developed and maintained throughout the A-123 process, such as implementation plans, test plans, corrective action plans, documentation of professional judgment decisions, etc.

⁴ Inherent risk statement – this is the statement of the perceived negative impact that could occur relative to an ECS sub-category or PCS Sub-Process activity, regardless of the presence of controls.

⁵ Entity Example 2

Example 2 – Segregation of Duties

Area: Control Activity

Sub-Category: Segregation of Duties

Risk Statement: An employee who creates a requisition and also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and / or abuse of government funds.

⁶ Inherent risk rating – this is the perceived likelihood and impact of a specified risk occurring in an environment absent of mitigating controls.

⁷ General Environment is not the control environment. General Environment would include things such as: number of cardholders in a Purchase Card Program; liquidity of assets at risk; stability of staff, etc.



A-123 Quick Start Guide – Documenting

⁸ Entity Example 2

Example 2 – Segregation of Duties

Area: Control Activity

Sub-Category: Segregation of Duties

Risk Statement: An employee who creates a requisition and also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and / or abuse of government funds.

Risk Likelihood: **HIGH – A decentralized organization with high turnover and a high number of requisitioning and approving officials.**

⁹ Entity Example 2

Example 2 – Segregation of Duties

Area: Control Activity

Sub-Category: Segregation of Duties

Risk Statement: An employee who creates a requisition and also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and / or abuse of government funds.

Risk Likelihood: HIGH – A decentralized organization with high turnover and a high number of requisitioning and approving officials.

Risk Impact: **LOW – Total annual requisitions are less than \$1M in a \$10B operation.**

¹⁰ Key controls are controls that have the greatest and the most critical impact in mitigating risk occurrence. For A-123, key controls are recorded in the AART as members of a control set. For both process and entity activities, there are likely to be numerous other controls that mitigate a specific risk; these should be maintained in Source Documentation.

¹¹ A preventive control is a control that reduces the likelihood and impact of a risk occurring. A detective control is a control that captures preventive control failures and/or early detection of risk occurrence.

¹² Entity Example 2

Example 2 – Segregation of Duties

Area: Control Activity

Sub-Category: Segregation of Duties

Risk Statement: An employee who creates a requisition and also approves the requisition, purchases the requested goods or services, and pays the subsequent invoice(s), resulting in fraud, waste, and / or abuse of government funds.

Risk Likelihood: HIGH – A decentralized organization with high turnover and a high number of requisitioning and approving officials.

Risk Impact: LOW – Total annual requisitions are less than \$1M in a \$10B operation.

Control Objective: **To prevent fraud, waste and/or abuse.**

Control Set: (1) Yearly issuance of a management statement highlighting the importance of internal controls including the segregation of duties in all business and financial activities. [P/Man] (2) Workflow technology is implemented to enforce limits of authority management. [P/Aut] (3) Security rules are set up such that no single user ID can be assigned the roles of creating a requisition and approving that requisition; approving a requisition and creating the corresponding Obligation; and creating the obligation and paying the invoice. [P/Aut] (4) Only 3 Administrators have the authorization to create and / or change security profiles and workflow rules. [P/Man] (5) Workflow technology is implemented to automate work flow message distribution to monitor expenditures and approvals. [D/Pau]

¹³ A preventive control is a control that reduces the likelihood and impact of a risk occurring. A detective control is a control that captures preventive control failures and/or early detection of risk occurrence.

¹⁴ Source Documentation includes policies, procedures, process maps, and other documentation created or maintained inside and outside of the A-123 program which supports the identified Areas / Sub-Categories, Processes / Sub-Processes, Risks and Controls. Testing plans, rating rationale details, or any other



A-123 Quick Start Guide – Documenting

documentation used to support an A-123 related decision are included as part of the [A-123 Detailed Documentation](#).

¹⁵ Activities are the lowest level of the decomposition of sub-processes and represent the actual steps and/or transactions executed. Risks typically are associated with activities.

¹⁶ Key considerations that should be considered for PCS in relation to PERCV:

- Risks affecting Presentation and disclosure– the particular components of the financial statements are properly classified described and disclosed.
- Risks affecting Existence or occurrence – an entity's assets or liabilities exist at a given date and recorded transactions have occurred during a given period.
- Risks affecting Rights and obligations – assets are the rights of the entity and liabilities are the obligations of the entity at a given date.
- Risks affecting Completeness and accuracy – all transactions and accounts that should be presented in the financial statements are so included
- Risks affecting Valuation or allocation – asset, liability, revenue and expense components have been included in the financial statements at appropriate amounts.

¹⁷ Process Example Invoice Risk Statement

Example 2 - Invoice

Process: Payable Management

Sub-Process: Invoice

Risk Statement 3: An invoice may be paid without receipt of goods or services, resulting in loss to the Government.

¹⁸ Process Example Invoice Likelihood

Example 2 - Invoice

Process: Payable Management

Sub-Process: Invoice

Risk Statement 3: An invoice may be paid without receipt of goods or services, resulting in loss to the Government.

Likelihood: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month related to the purchase of highly liquid assets (e.g. PCs, Software, PDAs, etc.).

¹⁹ Process Example Invoice Impact

Example 2 - Invoice

Process: Payable Management

Sub-Process: Invoice

Risk Statement 3: An invoice may be paid without receipt of goods or services, resulting in loss to the Government.

Likelihood: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month related to the purchase of highly liquid assets (e.g. PCs, Software, PDAs, etc.).

Impact: HIGH - Purchasing is the primary business activity and 90% of revenue results from the re-sale of procured goods.

²⁰ Key controls are controls that have the greatest and the most critical impact in mitigating risk occurrence. For A-123 key controls are recorded in the AART and are treated as a control set. For both process and entity activities, there are likely to be numerous other controls that mitigate a specific risk; these should be maintained in Source Documentation.

²¹ A preventive control is a control that reduces the likelihood and impact of a risk occurring. A detective control is a control that captures preventive control failures and/or early detection of risk occurrence.



A-123 Quick Start Guide – Documenting

²² Process Example Invoice Control Sets

Example 2 - Invoice

Process: Payable Management

Sub-Process: Invoice

Risk Statement 3: An invoice may be paid without receipt of goods or services, resulting in loss to the Government.

Likelihood: HIGH - Payments relate to a decentralized business unit with multiple payment locations and thousands of payment transactions per month related to the purchase of highly liquid assets (e.g. PCs, Software, PDAs, etc.).

Impact: HIGH - Purchasing is the primary business activity and 90% of revenue results from the re-sale of procured goods.

Control Objective: To prevent loss of funds.

Control Set: (1) Goods and / or services received are posted to contract in receiving system which updates accounting system. [P/Pau] (2) Invoice is posted to contract and is automatically placed on hold if the goods and / or services have not been posted. [P/Aut] (3) If the invoice is in excess of the amount posted for receipt of goods and / or services, the invoice is placed on hold. [P/Aut] (4) An e-mail notification is sent to appropriate parties advising them that the invoice has been placed on hold and the reason for the hold. [P/Pau]