

Entity Controls: Risk Matrix

Area	Sub-Category	Possible Entity Risks
Control Environment <i>A positive control environment is the foundation for all other internal control standards. It provides discipline and structure as well as the climate which influences the quality of internal control.</i>	Integrity and Ethical Values	Integrity and ethical values are not maintained and demonstrated by management and staff
		Agency management does not play a key role in providing leadership in the area of integrity and ethical values
		The agency does not have a positive "ethical tone"
		The agency does not provide guidance for proper behavior
		The agency does not provide guidance for removing temptations for unethical behavior
		The agency does not provide guidance for disciplinary actions, when appropriate
	Management's Commitment to Competence	Personnel do not possess and maintain the level of competence that allows them to accomplish their assigned duties
		Personnel do not understand the importance of developing and implementing good internal control
		Management has not identified appropriate knowledge and skills needed for various jobs
		Management does not provide needed training
		Management does not provide candid and constructive counseling
		Management does not provide performance appraisals
	Management Philosophy & Operating Style	Management takes too much risk
		Management has not adopted performance-based management
		Management has a dismissive attitude toward information systems
		Management has a dismissive attitude toward accounting functions
		Management has a dismissive attitude toward personnel functions
		Management has a dismissive attitude toward monitoring functions activities
		Management has a dismissive attitude toward audits and evaluations
		Management does not have a good relationship with Congress
		Management does not have a good relationship with central oversight agencies such as OMB
	Management does not have a good relationship with the OIG	
	Organizational Structure	The agency's organizational structure does not provide a framework for planning, directing, and controlling operations to achieve agency objectives
The agency's organization structure does not define key areas of authority and responsibility		
The agency's organization structure does not establish appropriate lines of reporting		
Assignment of Authority & Responsibility	The agency does not have procedures in place to delegate authority and responsibility	
	The agency does not have documented procedures in place to delegate authority and responsibility	



Entity Controls: Risk Matrix

Area	Sub-Category	Possible Entity Risks
		Agency delegation procedures do not cover authority and responsibility for operating activities
		Agency delegation procedures do not cover authority and responsibility for reporting relationships
		Agency delegation procedures do not cover authority and responsibility for authorization protocols
	Human Resources Policies & Practices	The agency does not have appropriate practices for hiring personnel
		The agency does not have appropriate practices for orienting personnel
		The agency does not have appropriate practices for training personnel
		The agency does not have appropriate practices for evaluating personnel
		The agency does not have appropriate practices for counseling personnel
		The agency does not have appropriate practices for promoting personnel
		The agency does not have appropriate practices for compensating personnel
The agency does not have appropriate practices for disciplining personnel		
The agency does not provide a proper amount of supervision		
Relationship with Oversight Agencies	Relationships between oversight agencies and management do not exist.	
Control Activities <i>Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives. Control activities occur at all levels and functions of an agency.</i>	Appropriate Documentation of Transactions and Internal Control Exist	The agency does not maintain physical control of, and properly secures/safeguard, vulnerable assets
		Recording of transactions and events are not done in a timely and/or accurate manner
		Access to resources and records is not limited to authorized individuals
		Accountability for custody and use of resources and records is not assigned and/or maintained
		Internal control, all transactions, and other significant events are not clearly documented
	Top Level Reviews of Actual Performance	Management does not track major agency achievements
		Management does not effectively manage its workforce
	Accurate and Timely Recording of Transactions and Events	Management does not maintain effective controls over information processing
	Reviews by Management at the Functional or Activity Level	Management does not compare actual performance to planned or expected results and analyze significant differences
		The agency has not established, and/or does not regularly review, performance measures and indicators
	Segregation of Duties	The agency has not properly segregated key duties and responsibilities
		Employees are authorizing and executing transactions and other significant events outside the scope of their authority
	Access Restrictions to and Accountability for Resources and Records	Documentation is not readily available for examination
Physical Control Over Vulnerable Assets	Information systems lack general controls	
	Information systems lack application controls	



Entity Controls: Risk Matrix

Area	Sub-Category	Possible Entity Risks
	Management of Human Capital	Management does not hire the right personnel for the job.
		Management does not provide adequate tools for the personnel to ensure job success.
		Management does not provide adequate training for the personnel to ensure job success.
		Management does not provide adequate incentives for the personnel to ensure job success.
		Management does not continually assess personnel skills.
		Management does not provide qualified and continuous supervision of internal control objectives.
		Management does not retain valuable personnel.
		Management does not plan for personnel replacement.
	Controls over Information Processing	Data entry edit checks are not conducted.
		Transactions are not accounted for using numerical sequences.
		Access to data, files, and programs are not controlled.
	Establishment and Review of Performance Measures and Indicators	Analysis cannot be conducted due to inconsistent or nonexistent performance indicators.
	Proper Execution of Transactions and Events	Personnel are unclear of levels of authority.
		Personnel enter into contracts or agreements that are beyond their scope of authority.
	Accurate and Timely Recording of Transactions and Events	Transactions are not entered in a timely manner
	Information Systems - General Controls	The agency does not have a corporate information systems architecture
		The agency is developing information systems outside of the corporate architecture
The agency has and/or is developing duplicative information system capabilities		
Information Systems - Application Controls	The agency does not have disaster recovery plans in place	
	Management has not recently revisited the sufficiency of disaster recovery plans	
Information & Communication <i>An agency must have relevant, reliable, and timely communications relating to internal and external events in order to properly run and control its operations. Information is needed throughout the agency to achieve all of its objectives.</i>	Internal relevant, reliable, and timely communications	Information does not generally flow down, across, and up the agency
		Management does not have access to operational and/or financial data
		Pertinent operational and/or financial information is not identified, captured, and distributed in a form and time frame that permits employees to perform their duties efficiently
	External relevant, reliable, and timely communications	There is a lack of adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals



Entity Controls: Risk Matrix

Area	Sub-Category	Possible Entity Risks
Risk Assessment <i>Internal controls provide for an assessment of the risks an Agency faces from both external and internal sources.</i>	Clear, Consistent Agency Objectives	Management has not established clear, consistent Agency objectives
		Management has not established clear, consistent objectives at the activity-level
	Identify Risks and Risk Factors, Internal and External	Management has not comprehensively identified risks at the Agency-level
		Management has not comprehensively identified risks at the activity-level
		Management has not considered all significant interactions between the entity and other parties
		Management has not considered all significant internal factors at the entity-level
		Management has not considered all significant interactions between individual activities and other parties
		Management has not considered all significant internal factors at the activity-level
	Risk Analysis and Actions	Management does not assess risk significance
		Management does not assess the likelihood of risk occurrence
		Management does not assess what actions should be taken to mitigate risks
		Management does not manage risk
		Management does not have mechanisms in place to identify and deal with risks that are unique to the operating environment of the Government
Monitoring <i>Internal control monitoring assesses the quality of performance over time and ensures that the findings of audits and other reviews are promptly resolved.</i>	Regular Management and Supervisory Activities	Ongoing monitoring does not occur in the course of normal operations
		Monitoring efforts do not include regular management and supervisory activities
		Monitoring efforts do not include comparisons, reconciliations, and other actions that people take in performing their duties
		Deficiencies found during ongoing monitoring are not communicated to the individual responsible for the function
		Deficiencies found during ongoing monitoring are not communicated to at least one level of management above the individual responsible for the function
		Serious matters found during ongoing monitoring are not reported to top management
	Separate evaluations of Controls	There are no separate evaluations of internal control effectiveness
		Separate evaluations of controls do not focus directly on their effectiveness at a specific time



Entity Controls: Risk Matrix

Area	Sub-Category	Possible Entity Risks
		The scope and frequency of separate evaluations do not take into consideration the assessment of risks and the effectiveness of ongoing monitoring procedures
		Deficiencies found during separate evaluations are not communicated to the individual responsible for the function
		Deficiencies found during separate evaluations are not communicated to at least one level of management above the individual responsible for the function
		Serious matters found during separate evaluations are not reported to top management
	Policies and Procedures for Audit Findings	Policies and procedures have not been established for ensuring that findings of audits and other reviews are promptly resolved
	Review and Evaluate Findings	Management does not promptly evaluate findings from audits and other reviews
	Develop Action Plan in Response to Findings	Management does not determine the proper actions in response to findings and recommendations from audits and other reviews
	Complete Findings Action Plan	Management does not complete, within established timeframes, all actions that correct or otherwise resolve the matters brought to management's attention

Notes:

- This is a listing of possible Entity Control risks. It is not necessarily all-inclusive of every possible risk that may impact an Entity Control area or sub-category.
- The term "agency" in this context means not only the organization as a whole, but also distinct sub-components of the organization.
- This information was derived from Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1, November 1999).

It is recommended that these Standards be reviewed for more detailed information on Entity Controls.

