STATE OF MISSISSIPPI
DEPARTMENT OF FINANCE AND ADMINISTRATION

TOPIC	INTERNAL CONTROL	SUB-SECTION 30.30.20
SECTION	COMPONENTS	ISSUANCE DATE JUNE 30, 2008
SUB-SECTION	RISK ASSESSMENT	REVISED - 2018

RISK ASSESSMENT

Risk affects an agency's ability to survive, to maintain its positive image, and to offer quality services and staff. Every agency faces a variety of risks from external and internal sources that must be assessed. Risk analysis involves a careful, rational process of estimating the significance of a risk, assessing the likelihood of its occurrence, and considering what actions and controls are necessary to manage it. Risk analysis also involves estimating the cost to the agency if an unexpected risk actually occurs. That analysis is based on the agency's assumptions about the risk and the costs associated with reducing it. Sometimes an actual risk may appear to require one set of actions, but the perceived risk, coupled with media reaction to that risk, requires another more expensive set of actions.

Risk assessment begins with the identification of the agency's primary responsibilities and functions through the development of an agency mission statement and strategic plan. In order to communicate the agency's mission statement and goals, risks must be identified both externally and internally.

External influences that contribute to risk include:

- Economic conditions
- Social conditions
- Political conditions
- External regulation
- Natural events
- Supply sources
- Technology changes

Internal influences that contribute to risk include:

- Changes in personnel duties (such as retention of key management personnel)
- Availability of funds for new initiatives or continuation of key programs
- Employee relations (such as compensation and benefit programs)
- Information systems (such as adequate backup systems)
- Data processing (such as disclosure of data, date integrity, and error, fraud or misuse of data)
- Cash management activities
- Asset protection and preservation

An agency's executive director and managers most often define organizational goals. Their management styles and the agency's mission will influence whether they use a formal, highly structured objective-setting process, or a more informal one. The goal of setting objectives is to develop a broadly stated strategic plan, allocating resources and establishing priorities. Senior management then defines specific objectives for various activities. The objectives of all the activities need to complement one another, while taking into account staff and resource capacities. Similarly, the programmatic goals of the smallest unit need to be consistent with the agency's overall strategic plan.
Once the agency develops a mission statement, the objectives of the agency's functions must be identified. They consist of the following three categories: operations, financial and compliance. Objectives often overlap. For example, an objective can serve as an operations objective and serve as a compliance objective.

Operations objectives help staff achieve the agency's basic mission or statutory responsibilities. An example would be the capital police officers patrolling the grounds of the state capital complex.

TOPIC	INTERNAL CONTROL	SUB-SECTION 30.30.20
SECTION	COMPONENTS	ISSUANCE DATE JUNE 30, 2008
SUB-SECTION	RISK ASSESSMENT	REVISED - 2018

Financial objectives set standards to assess management's performance, allocate resources, produce statistics, and protect assets. An example would be an agency developing its budget for LBO and DFA.

Compliance objectives include public obligations as well as operational practices, as defined by federal, state, and local laws, rules, and regulations. An example would be the Public Service Commission setting utility rates to meet both its obligation to protect the public interest and its statutory rate-setting responsibilities.

In risk assessment, management considers the mix of potential events relevant to the agency and its activities in the context of the agency's risk profile, which includes size, operational complexity, and regulatory restraints. Many events are routine, recurring, and already addressed in management's programs and operating budgets. Management must assess the risk of unexpected potential events and any expected events that could have a significant impact. Risk assessment is a continuous and repetitive interplay of actions occurring throughout the agency.

Agency heads may not take risks that would knowingly jeopardize their ability to meet obligations for financial management, financial reporting, or compliance with laws, regulations, policies, and procedures. Financial and compliance objectives serve needs of both the agency and of the State as a whole and are "not negotiable" when choosing strategies or tactics for achieving program objectives. Agency heads may only accept risk that relates to operational objectives, not risk that relates to financial or compliance objectives.

Management should assess the positive and negative impacts of potential events. The assessment should be based on the "the odds" that a given event will occur, and on the measurement of the effect of the event in quantitative or qualitative terms. This is known as likelihood and impact, respectively. Often, likelihood and impact estimates are based on past events, offering some objectivity.

Risks should be assessed on both an inherent and residual basis. Inherent risk occurs when management takes no action to reduce either the likelihood or impact of an event. Management assesses inherent risk and then decides how it will respond. Residual risk is the risk that remains after management's risk response.

Response to risk is divided into four categories:

Avoiding risk - ending those activities that give rise to risk; for example, eliminating a service or division.

Reducing risk - implementing everyday management decisions including setting control activities. For example, routine mechanical maintenance decreases the likelihood of a major computer hardware failure. Routine backups decrease the impact of technology equipment failure on the agency's ability to provide services.

Sharing risk - transferring a portion of likelihood or impact to another party. Examples of sharing include acquiring insurance or outsourcing an activity.

Acceptance risk - deciding to accept a risk because of cost or other considerations.

Once risks are identified, management considers their significance, the likelihood of their occurrence, and how they should be managed. Management may initiate plans, programs, or actions to address specific risks. When identifying risks, management should take into account relevant interactions within the agency as well as with outside organizations. Risks in different activities may be within their respective managers' acceptable risk levels but, taken together, may exceed the agency-wide acceptable risk level. In such cases, additional or different responses are needed to bring risk within the agency's acceptable risk level.

TOPIC	INTERNAL CONTROL	SUB-SECTION 30.30.20
SECTION	COMPONENTS	ISSUANCE DATE JUNE 30, 2008
SUB-SECTION	RISK ASSESSMENT	REVISED - 2018

The basic concepts of the risk assessment process should be present in every entity, regardless of size. However, the process is likely to be less formal and less structured in small and midsized agencies. All agencies should have established financial operations objectives. In the past, these may have been recognized implicitly rather than explicitly. The process of risk assessment as it relates to an agency's internal control plan provides the agency with the opportunity to review, revise, and explicitly recognize these objectives.

An agency's risk assessment process regarding financial objectives should consider the events and circumstances that may occur and adversely affect its ability to record, process, summarize and report financial information. Management should also consider previous findings; e.g., auditor identified, internal management reviews, or other identified noncompliance with laws and regulations. Management should also identify and react to dramatic changes possibly having a persuasive effect on the agency, such as:

- Changed operating environment
- Significant shifts in the workforce
- New or redesigned information systems
- New personnel
- New services, products, activities, or acquisitions
- Organizational restructuring or reductions
- Decentralized operations
- New technology
- Rapid growth

Management should identify the transaction cycles comprising the agency's overall accounting system. An agency can identify its transaction cycles by connecting the financial transactions it uses to the function of the transactions within the agency's accounting system. This process involves listing all of the transactions that an agency must initiate to perform its function, determining relationships between transaction types, and grouping related transactions into cycles. Common transaction cycles within MAGIC include:

Transaction Cycle	Examples of Transactions	Possible MAGIC Documents
Grants	Grant awards, receipts and disbursements	XG,YF,YG,ZG,ZI
Purchases	Requesting Goods or Services	WA,WE,WI
Vendor Invoice and Disbursements	Payment for Goods or Services	KR,KG,PC,RE,KP
Customer Billing and Receipts	Revenue Processing	DZ,DG,YC,YZ
General Accounting	Miscellaneous Entries	ZE,ZT,YV,ZZ
Inter-agency	Billings and Receipts	YS,YT,YU
Assets	Asset Posting and Depreciation	AA,AF,AS,ZA
Payroll and Travel	Payment of Employees Payment of travel to employees	Through SPAHRS

TOPIC	INTERNAL CONTROL	SUB-SECTION 30.30.20
SECTION	COMPONENTS	ISSUANCE DATE JUNE 30, 2008
SUB-SECTION	RISK ASSESSMENT	REVISED - 2018

Risk ranking factors should be applied to each transaction cycle to identify those with the greatest risk. Risk is defined as the level of vulnerability to fraud, abuse, and mismanagement. Factors considered should include magnitude of funds involved, potential impact of ineffective operation, sources of input, degree of automation, known problems, and prior audits. An agency should document the results of this analysis in its internal control plan. An explanation of how the internal control process is organized to address these risks should also be documented.

The management of these risks via the internal control structure should provide reasonable assurance that financial processing functions work as intended.