RISK ASSESSMENT

We face a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

There are risks inherent in any activity. Smart managers know the potential impact and likelihood of occurrence of any number of risks, and put in place cost-effective controls to manage those risks. **External risks** such as vendor fraud could compromise health and safety of staff, clients, students, patients, customers. **Internal risks** such as employee incompetence, unsafe buildings or ailing computer systems also imperil an organization.

Simply put, when we allocate resources to meet a legislative mandate or program objective, we must be mindful of two things:

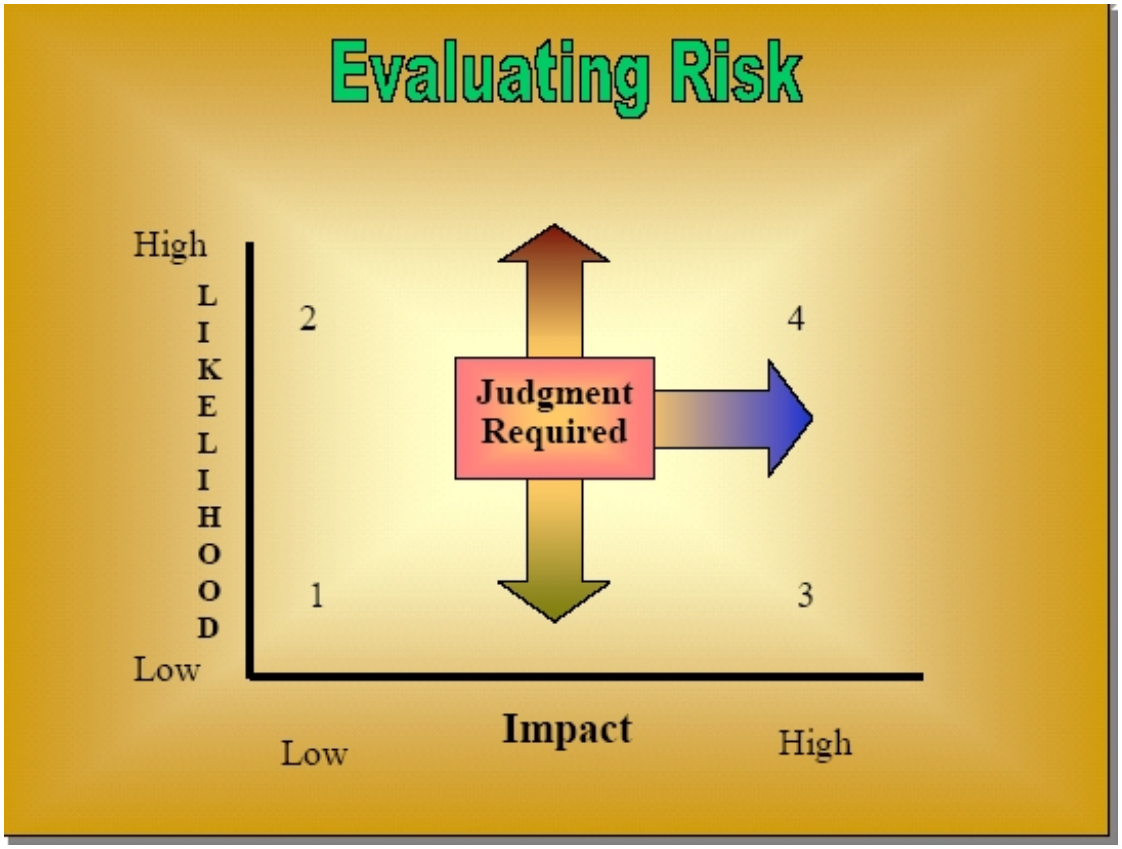
- What are we trying to achieve?
- What are we trying to avoid?

The first consideration requires us to define concrete, tangible objectives – which can be measured objectively - not subjectively. For example standardized testing of a student before AND after a program has been conducted can determine if there was any improvement in attitude, understanding or scholastic performance. Routine blood tests can tell a lot about a patient's health, diet, susceptibility to various diseases, or compliance with a rehabilitation program.

The second consideration requires us to identify the kinds of risks that could interfere with our achievement of those objectives. Fraud, waste and mismanagement come to mind, but there are also "inherent risks" that come with the territory, requiring management controls to minimize or manage such risks in a cost-effective way. Keeping medicines and toxic materials away from toddlers is one low-cost, common sense approach to minimizing the risk of poisoning. Guarding personal financial information is certainly in the news these days as criminal element twist the new technology to defraud the unsuspecting.

Risk assessment is a management process involving input from those involved in administering a program. It may even involve input from those served by a program.

Risks are ranked by **Probability** (likelihood of occurrence) and **Impact** (Severity or affect on people, resources, reputations, etc.). The following chart (or a variation of it) has been adopted by every management group concerned with program effectiveness and risk management:



Source: *OSC Standards for Internal Control in NYS Government*

The chart is divided into four quadrants. Risks of low probability and little impact (quadrant 1) require very little attention. Risks in quadrant 2 – even if a frequent occurrence require little attention, because of minimal impact. We cannot afford to spend disproportionate amounts to control insignificant risks. Imagine the cost for equipment (and cost to employee morale) if we were to put inventory control tags on every pen and pencil used in the office.

Ask yourself *"If something could go wrong in any activity, how serious would the consequences be?"* In some instances you may be able to place a dollar value on the impact of failure. In other instances you may be able to assess a consequence in terms of the health and/or safety of human lives under our responsibility.

RATING YOUR VULNERABILITY

We have identified twelve characteristics of vulnerability (risk) which apply to any human endeavor – government or private sector, non-profit or commercial. A careful consideration of each characteristic can help you determine if the management controls you have in place are proportionate to the risk, and appropriate to the environment. One hit: almost all of these depend on human beings, be it competent staff, honest vendors, or sincere citizens who depend on success.

A. TWELVE CHARACTERISTICS

To arrive at an overall understanding of the risks inherent in your function(s) you need to assess the following **areas of vulnerability**:

1. Operational Stability
2. Organizational Structure
3. Policies & Procedures
4. Sensitivity/Complexity of Operations
5. Personnel
6. Financial Assets
7. Physical Assets
8. Authorizations
9. Frequency of Reviews
10. Reliance on Information Systems
11. Influence
12. Impact of Failure

See following pages for definitions and examples of each characteristic

Each of these areas needs to be evaluated for the risks inherent in your organization, related to the specific function under your supervision. An overall rating of **High**, **Moderate** or **Low** risk is derived from a combination of these twelve risk assessments.

B. HOW VULNERABLE ARE YOU?

Using a **rating system** from 1 to 5 - with *1* being the *lowest* risk, and ***5*** being the ***highest*** risk, let us consider the previous example of our sample function (found on Page 2 of this Guide), then go on to rate the vulnerability of one of your own functions.

Functions with *HIGH* vulnerability may be characterized by complex/sensitive operations, with high staff turnover, handling significant cash receipts. Failure to prevent or detect misuse of assets can seriously damage the agency's reputation and mission.

Functions with *LOW* vulnerability rely on qualified/trained staff, provide good documentation of policies & procedures and are subject to frequent outside review of operations. Potential for misuse of significant assets is low, or may not reflect directly on the agency's reputation and mission.

C. VULNERABILITY ATTRIBUTES

CHARACTERISTIC:	CONSIDERATIONS:
1. Operational Stability: If the function has existed for some time with the same fundamental mission, without major new responsibilities, legislative mandates or personnel changes, the risk is *Low*. *(Frequency of change increases the risk)*	Does this function involve a long-term stable program, or a brand-new mandate/activity? Are staff well-seasoned in this operation, or has there been considerable turnover of veteran staff or acquisition of new personnel?
2. Organizational Structure: If the organizational structure is well-documented & periodically reviewed, with clearly defined areas of authority, and direct and indirect lines of supervision are established & understood, the risk is *Low* *(As the structure becomes more decentralized, the risk increases).*	Are organizations charts up-to-date? Are individual unit functions well-documented? Are staff clear as to lines of authority and in-house clearance mechanisms? Does the organization include field staff operating with limited supervision? Is individual employee productivity and attendance reviewed adequately?
3. Policies & Procedures: If policies & procedures for the function are documented, updated, and they clearly define employee responsibility & limits of authority, the risk is *Low*. *(The better the documentation, the lower the risk)*	Are policies & procedures clear and current? Is there potential for conflict or confusion with other policies or higher level authorities? Do employees have authority commensurate with responsibility, to ensure they can do their job in a timely, accountable manner? Are procedures keeping pace with organizational change or new mandates?
4. Sensitivity/Complexity of Operations: If the function is important to the agency's primary responsibilities; and involves sensitive program, fiscal, or political considerations; or is highly technical or administratively complex, the risk is *High*. *(Greater complexity implies greater risk)*	Is the function routine/repetitive, involving large numbers of small-value transactions, or does it involve a complex set of tasks, requiring individual initiative and/or involvement of other bureaus or other agencies? Is this function highly visible/vital to local political jurisdictions or the public?
5. Personnel: If properly trained & technically proficient personnel are assigned to this function, assignments are clearly defined, employee performance is periodically reviewed, and additional staff development is provided as necessary, the risk is *Low*. *(The more qualified & trained the staff, the lower the risk).*	Are staff adequately trained to conduct the variety, and complexity of functions? Are special credentials /training a prerequisite for employment? Is there a viable, ongoing staff development program to keep employee skills current with administrative systems, computer support or emerging new mandates?
6. Financial Assets: If the function requires accurate & comprehensive financial records to handle significant cash receipts, disbursements, and negotiable instruments, or it has a large operating budget, the risk is *High*. *(More handling of funds means greater risk)*	Does this function involve handling of cash or negotiable instruments (checks)? Is there adequate separation of duties to ensure accuracy/accountability? Is supervision/oversight commensurate with the value of assets received/disbursed (e.g. foster parent checks, youth allowances, petty cash payments)?

CHARACTERISTICS:	CONSIDERATIONS:
7. Physical Assets: If the function maintains an inventory of or utilizes expensive or transportable physical assets which could be lost, stolen, or damaged, the risk is *High*. *(Risk is also increased if comprehensive inventories are not maintained.)*	What is the dollar value of assets used/accessed by this function? What potential is there for individuals to misuse such assets for personal gain (e.g. long distance phone calls, pilfering of office supplies/foodstuffs or theft of computers / electronics/ vehicles)?
8. Authorizations: If the function involves approving applications, certifications or contracts; or requires on-site inspection of facilities, the risk is *High.* *(The greater the involvement, the higher the risk.)*	Does this function involve approving service contracts, certification of building/construction safety, or vendor contracts? Does agency staff directly inspect facility or service provider sites? Would the consequences of staff action be significant enough to tempt desperate or unscrupulous parties to offer inducements for overlooking shortcomings?
9. Frequency of Reviews: If the function is subject to frequent outside reviews of operations by agency internal auditors, outside auditors, accreditation groups or other oversight bodies, the risk is *Low*. *(Fewer reviews & less follow-up means greater the risk)*	Is this function scrutinized on an annual basis, or could many years elapse before a potential problem is detected? Where errors are detected, is corrective action pursued in a timely manner? Are findings of auditors or oversight bodies made public (or disseminated beyond the individual unit affected)?
10. Reliance on Information Systems: If the function relies on (or is responsible for) computer-generated information or statistical data - either electronic or hard copy - which must be accurate, complete & protected from unauthorized use, the risk is *High*. *(More reliance on, & complexity of, statistical information means greater risk.)*	Could improper access to information damage individuals or the agency's reputation? If information systems were compromised, is there potential for personal financial gain, or sabotage of a vital agency function? Are there manual backup systems & procedures available to reconstruct files (disaster recovery)?
11. Influence: If the function is subject to external influence by interest groups and/or private interests with the potential for conflicts of interest by administrators/employees, or pressure for untimely action, the risk is *High*. *(More interest group contact means greater risk).*	Is this function of interest to legislators, local elected officials, community organizations or special interest groups? Are steps taken to minimize potential for conflict of interest by the agency's own staff? Does the administrative organization screen line staff from undue pressure/influence?
12. Impact of Failure: If the function should fail to operate properly, with serious fiscal or human consequences, or if the internal controls should fail to detect the misuse or misappropriation of assets by employees or agency-funded programs, the risk is *High.* *(Greater significance means greater risk.)*	If something goes wrong in this function, is their serious risk of personal harm to staff or clients (e.g. client abuse, disease contagion, accident or fire), or significant misuse of agency assets by staff or agency-funded programs? What dollar value could be placed on such system failure? Is there potential for a lawsuit (involving a significant monetary award or damage to agency's reputation)?

FUNCTIONAL VULNERABILITY ASSESSMENT – 2009

Program/Function: _____

Bureau/Unit: _____

Instructions: For each characteristic below, rate vulnerability from 1 to 5 - with 1 being the lowest risk, and 5 being the highest degree of risk.

	Characteristic	*1 -Low Risk*	*2 – Low to Moderate*	*3 - Moderate Risk*	*4 – Moderate to High*	*5 -High Risk*
1.	**Operational Stability**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
2.	**Organizational Structure**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
3.	**Policies & Procedures**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
4.	**Sensitive/Complex Operations**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
5.	**Personnel**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
6.	**Financial Assets**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
7.	**Physical Assets**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
8.	**Authorizations**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
9.	**Frequency of Reviews**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
10.	**Reliance on Information Systems**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
11.	**Influence**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
12.	**Impact of Failure**	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

TOTAL *(Add ratings 1 thru 12)* Score: _____

Total Score of 48+ indicates
☐ **HIGH Vulnerability**

Total Score of 25-47 indicates
☐ **MODERATE Vulnerability**

Total Score under 25 indicates
☐ **LOW Vulnerability**

Completed By: _____ **Date:** _____

Reviewed By: _____ **Date:** _____