

Risk Assessment Matrix (RAM) Process

Risk assessment is the process by which businesses and organizations focus on critical areas of concern and prioritize their use of resources in order to maximize response and recovery efforts. In making strategic decisions, business and government leaders routinely try to predict the benefits and/or harm that might be caused by implementing or failing to implement those decisions. The Risk Assessment Matrix (RAM) can be viewed as a logical extension of that process.

Through this process, companies and agencies:

- Identify their most important (critical) processes and functions;
- Identify threats most likely to impact those processes and functions;
- Determine the vulnerability of critical functions and processes to those threats; and
- Prioritize deployment of personnel and resources in order to maintain continuous operation of critical functions and processes.

An accurate risk assessment can reveal operations that are subject to a “single point of failure.” Implementation of effective prevention measures will eliminate some threats and significantly reduce the impact of others. It has been reported that, for every \$1.00 spent on prevention, there is a potential savings of \$7.00.

Information collected using the RAM model will enable a business or agency to identify:

- Functions and processes critical to maintaining continuous operation;
- Threats most likely to disrupt those identified, critical functions and processes;
- Personnel and expertise required to handle critical incidents that impact the continuity of business and/or agency operations.

Areas to be considered include:

- Company/agency products and services and the facilities and equipment needed to produce them;
- Products and services provided by suppliers, especially sole source vendors; and
- Lifeline services such as electrical power, water, sewer, gas, telecommunications, and transportation.

Some of the data collected during the RAM process should be shared between public and private entities in order to facilitate effective public and private response. Ineffective response results in unintended impacts such as:

- Loss of business and tax revenue;
- Loss of customer and citizen confidence;
- Exposure to litigation;
- Bankruptcy; and
- Damage to business and community reputation/image.

Risk Assessment Matrix: A Flexible Tool

The RAM format is intended for use by private and public organizations of varying sizes and configurations. It is a concise, user-friendly tool for gathering information to prioritize assets, identify mitigation needs and develop preparedness, response, and recovery plans.

The six (6) steps in the RAM process are:

1. Identify *business functions and processes*.
2. Rank functions and processes according to *criticality*.
3. Determine *recovery time* required to sustain critical functions and processes.
4. Identify *threats* that impact each critical business function and process.
5. Determine the *vulnerability* of each critical business function and process.
6. Confirm that appropriate *personnel, plans, and resources* are in place to respond. If gaps exist, identify relevant *solution areas*¹ to address shortcomings.

The manner in which the RAM is completed will vary according to circumstances. A small business or agency may assign one individual to complete the process for the entire organization. A large, multi-divisional organization (shipping, human resources, operations/manufacturing, etc.) may wish to task an individual in each division or unit with assessing that part of the operations. Data collected is then used to establish critical incident response priorities.

Preliminary Information

Before focusing on specific functions, it is important to make sure that everyone in the organization sees the “big picture.” Those responsible for specific areas need to have a clear understanding of how their areas contribute to the bottom line of the organization. Corporations and agencies with a well-defined vision, mission statement and strategic plan are ready to initiate the RAM process. Other groups may need to spend some time in this area.

Following are the six (6) steps of the RAM model. Within the steps are “values” or explanations. Use the RAM worksheet to capture pertinent information².

Step One: Identify Functions and Processes

List the separate functions and processes required to create a product or provide a service. Typical business functions/procedures include:³

- Shipping & Receiving
- Inventory
- Service
- Human Resources
- Marketing
- Sales
- Communications
- Production
- Finance
- Training
- Facility Management
- Information Technology

¹ Planning, Organization, Facilities, Equipment, Training and Exercising.

² Detailed instructions are printed on the back side of each RAM form. A copy of the RAM is attached to this document.

³ This list is not all-inclusive. Make adjustments as necessary.

Step Two: Determine Criticality

Of the business processes listed in Step #1, which are the **most critical** to the continual operation of the business or agency? In determining criticality, consider the following:

- Does this business function affect the safety of employees or the general public?
- How important is this business function to the mission of the agency/business?
- How important is this function to the continuity of business operations?
- How would a loss or disruption affect the “bottom line?”

The following definitions may be used as a general guide and should be modified to meet the requirements of each specific process or function:

- *Critical* – necessary and/or vital. May pose a life-safety risk to employees and/or general public.
- *Essential* – important but not critical. Disruption would cause difficulties.
- *Non-Essential* – disruption is merely inconvenient.

Step Three: Determine Recovery Time

Determine the **recovery time** for each critical business function listed in Step #2. In determining recovery time, consider the following:

- Time from loss or disruption of process to the point when continued disruption or loss is detrimental to the mission of the business;
- Special circumstances that may delay or prevent recovery actions, i.e., designation of an area as a crime scene or contamination by a dangerous chemical;
- Impact on public confidence if response is perceived to be too slow.

In determining recovery time the following guide may be considered:⁴

- *Immediate* – 0 to 24 hours;
- *Delayed* – 24 hours to 7 days;
- *Deferred* – beyond 7 days.

Step Four: Identify Threats

Identify **threats** that may halt or disrupt each of the critical business functions identified in Step #3. This will likely require input from public agencies (law enforcement, fire services, emergency medical services, public works, local emergency management officials, etc.). Consider those threats that have occurred and those that may be likely to occur. Multiple threats may impact a single function or multiple functions. In identifying threats consider:

- Natural disasters (tornados, floods, severe weather);
- Human-caused events (workplace violence, terrorist attack, sabotage, critical information theft);
- Facility-related emergencies (hazardous materials, loss of utilities, proximity to other threats);
- Asset protection incidents (inadequate systems, untrained personnel);
- Information systems difficulties (lack of backup);
- Employee-related problems (training, attitude, misconduct/grievances);
- Other events and incidents (nearby threats, political activities).

⁴ Each business must determine their appropriate recovery criteria.

When assessing the various threats it is important to consider:

- 1) **What** can occur;
- 2) The **damage** it is likely to cause.

Step Five: Determine Vulnerability

Determine which of the threats identified above have the **greatest likelihood** of disrupting or attacking each critical business function. When assessing how vulnerable a process or function is to the various threats, it is important to consider:

- 1) How **likely** it is that a threat will occur;
- 2) How **often** a threat is likely to occur.

The following descriptions are suggested as a guide:

- *Highly Vulnerable* – business functions that are most likely to experience threat.
- *Vulnerable* – may experience the threat or threat.
- *Not Vulnerable* – not likely to experience the threat or threat.

Step Six: Select Action Plans

Determine if there are **appropriate plans**⁵ and **resources** to address the threats that are most disruptive to the critical business functions. It is imperative that these plans and capabilities are current and adequate⁶. If gaps or shortcomings are discovered, determine:

- What do I have and what do I need? Solution areas include:
 - Planning.
 - Facilities
 - Training.
 - Organization.
 - Equipment.
 - Exercising.
- Can the issues be addressed using available company personnel and resources or will outside personnel and/or resources be required of other businesses and/or public organizations?
- If solutions require coordination with public agencies, do the businesses and public agencies involved need to develop or enhance a public-private partnership?

Risk Assessment Matrix Form

A copy of the Risk Assessment Matrix Form is attached. There are further instructions for completing the RAM on the back side of the document.

Summary

The above process should result in a determination of 1) what is critical to the continual operation of the business or agency, 2) what is most likely to disrupt those critical business functions, and 3) if there are current and adequate response plans in place. The process involves determining priorities and allocating resources to assure continuity of critical operations.

⁵ This includes both private, business plans and public, emergency operations plans.

⁶ Plans and resources must be tested regularly by conducting tabletop, functional and full-scale exercises.

