The Resiliency Institute™ Index and Report

created for:

SAMPLE COMPANY

Table of Contents (Sample)

Table of Contents (Sample) 2

The Resiliency Institute™ Index and Report 4

Disclosure Statement 4

Confidentiality Notice 4

Copyright Notice 4

Resiliency: 4

The Resiliency Institute™ Index and Report 5

The Resiliency Institute™ Index 5

The Resiliency Institute™ Index Rating Table and Graph 5

Data Table and Normalized Chart 7

Section 1: Emergency Management 8

(There are 49 questions in this section. Below are a representative sample of the questions.) 8

Section 2: Corporate Crisis Communications 11

(There are 29 questions in this section. Below are a representative sample of the questions.) 11

Section 3: Facilities and Security Management 13

(There are 60 questions in this section. Below are a representative sample of the questions.) 13

Section 4: Operational Infrastructure 16

(There are 25 questions in this section) 16

Section 5: Technical Infrastructure 16

(There are 52 questions in this section) 16

Section 6: Human Resource Management 16

(There are 25 questions in this section) 16

Section 7: Continuity Management 16

(There are 26 questions in this section) 16

Section 8: Financial Control 16

(There are 14 questions in this section) 16

Section 9: Governance and Compliance 16

(There are 25 questions in this section) 16

Section 10: External Business Chains 16

(There are 21 questions in this section) 16

Section 11: Community and Environmental Stewardship 16

(There are 19 questions in this section) 16
Section 12: Risk Management and Control 16
(There are 20 questions in this section) 16
Closing Comments 17
Appendix A: Business Continuity Glossary *18*
Appendix B: Flood Plain Data *19*

The Resiliency Institute™ Index and Report

Disclosure Statement

The opinions expressed in this report are solely based on material and information supplied by the client. The SAMPLE COMPANY and The Resiliency Institute have not attempted to verify any of the information supplied. As such, all comments, opinions, and recommendations are offered as suggestions and discussion points.

Confidentiality Notice

Copyright Notice

Resiliency:

That quality of an organization's culture, procedures, training, awareness, and infrastructure that allows it to continue to meet operational goals even when impacted by a disruptive event.

The Resiliency Institute™ Index and Report

This report will give management insight into the ability of the organization to maintain an acceptable level of operational performance even in the face of extraordinary events. This analysis was sponsored by the who engaged the services of The Resiliency Institute, LLC to conduct this study.

Funding for this analysis is provided by SAMPLE COMPANY to help preserve human life, protect assets, and promote a healthy, resilient community.

The information used in this assessment is drawn from a self-assessment questionnaire completed and returned by the firm to the analysts at The Resiliency Institute for comment and reaction.

The material in this questionnaire is drawn from ongoing original research conducted by The Resiliency Institute and sponsored in part by SAMPLE COMPANY. For more information on the design of this self-assessment survey, please contact The Resiliency Institute directly.

The Resiliency Institute™ Index

The Resiliency Institute in collaboration with SAMPLE COMPANY and several business resiliency experts have developed a benchmarking tool that allows an organization to measure its level of crisis preparedness and project its ability to operate during a disruption. Known as The Resiliency Institute™ Index, this unique metric allows an organization to periodically measure its performance against recognized "best practices." By periodically consulting The Resiliency Institute™ Index, management can track the firm's performance in each of the twelve areas identified as critical to successful and sustained operations, and quickly address issues needing attention.

The Resiliency Institute™ Index Rating Table and Graph

The original self-assessment questionnaire solicited answers in twelve areas. These areas represent a superset of topics that are identified as critical to operations by the major industry standards in this area, such as NFPA 1600, SPC 1, and BS 25999.

This part of the report summarizes the resiliency rating of the firm based on the answers given to the questions in these twelve areas. These areas are identified as ones that either must continue to operate to maintain production, or that will be called upon to respond to a crisis. By measuring the resiliency of each of these twelve areas the resiliency index of the firm can be determined.

This information is presented as a table and as a bar-chart graph.

A quick review of these results will provide some insight into the firm's (and its local community's) readiness to respond in a resilient manner to a widespread event such as a regional power outage.

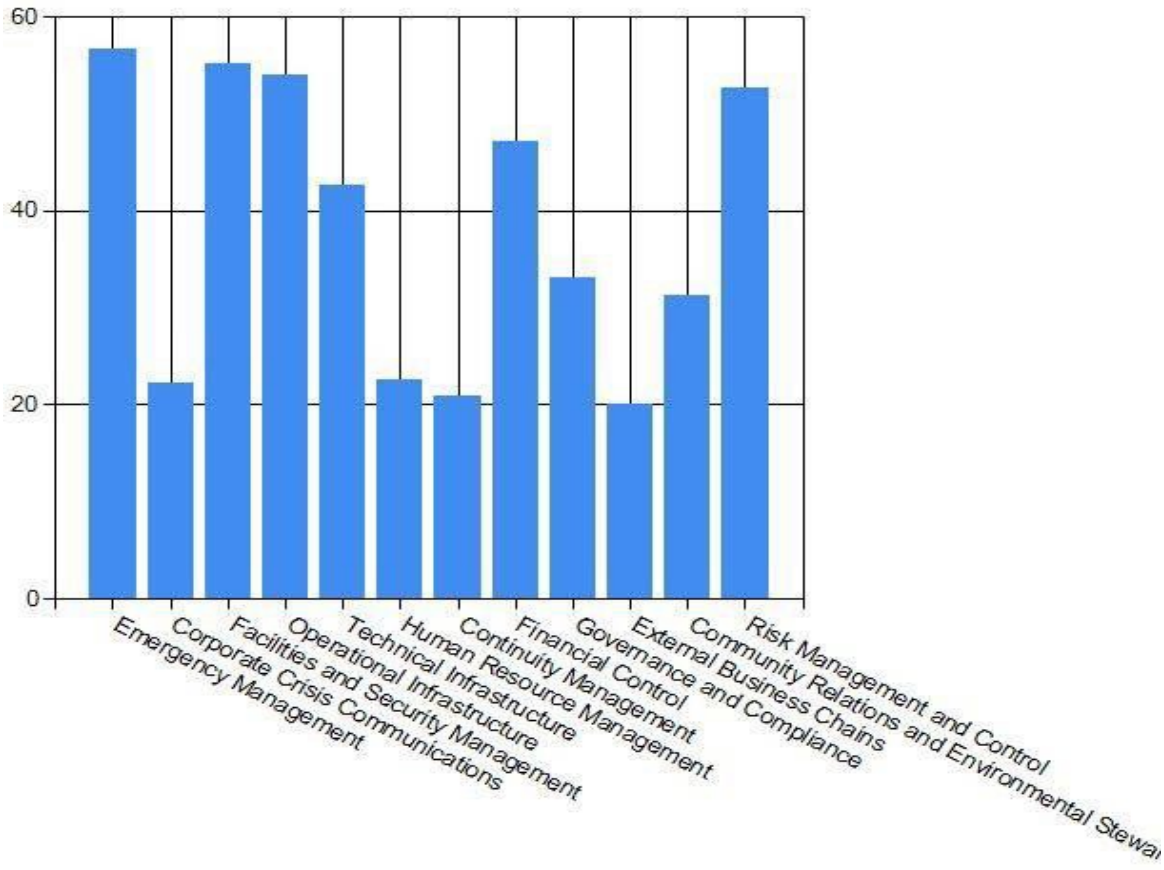
The twelve disciplines are:

- Emergency Management
- Corporate Crisis Communications
- Facilities and Security Management
- Operational Infrastructure
- Technical Infrastructure
- Human Resource Management
- Continuity Management
- Financial Control
- Governance and Compliance
- External Business Chains
- Community Relations and Environmental Stewardship
- Risk Management and Control

Clients are encouraged to take the survey often annually and track the changes in their resiliency rating as they implement various programs.

Data Table and Normalized Chart

Section	Max Score	Survey Score	Normalized Score
Section 1: Emergency Management	282	160.0	56.7%
Section 2: Crisis Communications	153	34.0	22.2%
Section 3: Facilities and Security	280	154.5	55.2%
Section 4: Operational Infrastructure	122	66.0	54.1%
Section 5: Technical Infrastructure	222	94.5	42.6%
Section 6: Human Resource	115	26.0	22.6%
Section 7: Continuity Management	136	28.5	21.0%
Section 8: Financial Control	89	42.0	47.2%
Section 9: Governance and Compliance	133	44.0	33.1%
Section 10: External Business Chains	107	21.5	20.1%
Section 11: Community and Environmental Stewardship	99	31.0	31.3%
Section 12: Risk Management and Control	77	40.5	52.6%



Section 1: Emergency Management

(There are 49 questions in this section. Below are a representative sample of the questions.)

Question #5: Have arrangements been made for the evacuation of disabled or special needs individuals?

General Comments: By law organizations must take into consideration the safety needs and requirements of all employees. This includes preparations for the health and safety of individuals who may require special assistance during a crisis. The Resiliency Institute recommends that the question of special assistance be included as part of new employee orientation. In this way, those who may require additional assistance can voluntarily identify themselves. Each time the EPP is reviewed and updated, this issue should be readdressed.

Selected Response: Yes

Recommendation: It should be gratifying that the organization has taken the requirements of all the employee's needs into consideration. Those who are not fully prepared and supported may not manage through a crisis well and all should be protected. It is recommended that all new employees discreetly be asked by HR professionals if there is some assistance they might require in an emergency. This can be difficult if not handled appropriately so it is suggested that trained or experienced staff be involved, and that privacy is ensured. We suggest also that you make a special effort each time the emergency preparedness plan is reviewed and updated to consider that some individual situations may have changed, or new employees may have a special need.

Question #6: Have rendezvous points been established, clearly marked and publicized?

General Comments: A concern of emergency workers is that it is possible to lose track of some individuals involved in a crisis. Fire, police and safety teams do not know if people are still in an emergency or not and this can cause potentially dangerous responses. It is important that each organization have a clearly defined, well-marked rendezvous location understood by all to be the place they must go during and after a crisis.

Selected Response: Yes

Recommendation: The Resiliency Institute recommends that training on the evacuation routes and rendezvous points be part of an annual exercise, such as a fire drill.

Question #7: Are the rendezvous points sheltered against the elements?

General Comments: A crisis can happen at any time of the year, including during inclement weather. For this reason, it is important to select a rendezvous point that is secure in every season.

Selected Response: Partially

Recommendation: This is an important issue and The Resiliency Institute recommends you complete your plans and designate such a site within the next three months. A common mistake in choosing an evacuation rendezvous site is to not factor in the need for shelter in inclement weather or sheltering as appropriate. Without a sheltered location it is doubtful that some people will show up and it is extremely difficult to hold a crowd together. Some organizations choose 2 sites: one for fair weather and an alternate. This does complicate matters since in a crisis people don't want a choice – they want direction. Selecting a protected site is an opportunity to put in place a mutual aid agreement with neighboring businesses. The Resiliency Institute understands that there are situations where it is not feasible to find a sheltered location. It is also important to try to select an easy-to-locate site since during a crisis people are easily distracted or confused. Explaining the location in terms of a landmark (e.g., "Meet underneath the flagpole," is a good practice. For more information on this topic, please contact The Resiliency Institute.

Question #8: Has the firm developed criteria for judging different levels of an emergency?

General Comments: The decision of how and when to react to a crisis must be appropriate to the incident's scale and severity. It is best practice to have defined criteria specifying the appropriate response. The danger of not having clearly defined, published and exercised criteria, is that the emergency will be improperly managed.

Selected Response: Yes

Recommendation: Many organizations establish a three, four, or five tier models to judge the severity of an incident. If you haven't done this, please give the idea of tiered response consideration. Small events like a wastebasket fire might simply be handled by an individual using a fire extinguisher, whereas a power outage might necessitate the mobilization of the whole response team. The Resiliency Institute recommends you consider developing a multi-tiered response model. For more information on this concept, contact M411 directly.

Question #9: Does the firm support community emergency preparation plans such as Community Emergency Response Team (C.E.R.T.) training?

General Comments: The CERT program (http://www.citizencorps.gov/cert/index.shtm) helps people prepare for hazards in their local community. Training includes basic disaster response skills, such as fire safety, search and rescue, team organization, and disaster-oriented medical operations. C.E.R.T. members assist others in the workplace when professional responders are not immediately available to help.

Selected Response: Yes

Recommendation: While not required by any law or regulation, supporting the CERT program has both positive community relations implications as well as helping your own organization be better prepared for an emergency. This is not an example of altruism, but common sense, because having well trained individuals in your organization will protect life

and property from more harm than may occur without this training. Additionally, it is very low cost, often free, and builds relationships with the local safety agencies such as fire, police and EMTs, further enhancing the ability of your organization to effectively respond to an emergency.

Section 2: Corporate Crisis Communications

(There are 29 questions in this section. Below are a representative sample of the questions.)

Question #1: Is there a documented plan for crisis communication designed to deal specifically with emergencies?

General Comments: During and immediately after a crisis, communications are essential. Most communication plans provide a way of passing information to employees and other stakeholders, usually through an internal public-address system or "call tree" (mostly for notification of off-premises personnel). All on-premises mechanisms should have at least two modes that are clear and very distinct: one that is used to notify people to leave the facility (evacuation as in the case of a fire) and a second that signals a shelter-in-place situation. Training on these two different systems should be conducted periodically and the responses to these very distinct messages monitored for correct reactions. Confusion in crisis situations is to be expected and the best way to reduce it is through training. These plans also address working with the media. For the latter, it is advised to have pre- developed background information on the organization and its management. Having such boilerplate documents will save time and provide a more accurate representation of your policies and culture. Beyond notification, these plans should also provide a mechanism for keeping interested stakeholders, including employee families, informed. Some organizations use a dedicated telephone line with a recorded message. Others additionally set up a private section of their website where information is posted. A third popular strategy is to hold a periodic conference call where new developments are reviewed, and questions answered. Clearly, the advantage of this last technique is that it provides a degree of interaction with the stakeholders. These communication methods can be implemented inexpensively. There are more sophisticated "notification and escalation" systems available which can increase the likelihood that critical messages are received. Please contact The Resiliency Institute for more information on these systems or with any questions related to crisis communications.

Selected Response: No

Recommendation: Not having a documented plan seriously impedes the effectiveness of your overall effort to achieve resiliency. The lack of a plan also has serious life-safety implications, especially if there is no onsite notification capability. When you eventually implement a crisis communication system, The Resiliency Institute suggests that you make a concerted effort to ensure a distinction between signaling an evacuation versus a shelter-in- place situation. The plan should set expectations on how long it takes to notify the target audience and an overall effectiveness goal. For example, internal public-address systems should have a goal of 100% coverage of the facility while a call tree program may expect to reach 80% of the people on the first call, an additional 15 % with a follow up call and the last 5% on a third or subsequent call. If your organization suffers from high turnover, or is expanding rapidly keeping contact

information current can be a challenge and merits frequent review, perhaps as often as quarterly or monthly. Given the important life-safety implications of this portion of the resiliency plan The Resiliency Institute urges you to implement such a system within the next three months.

Question #2: Has the crisis communication plan been reviewed and updated within the past 12 months?

General Comments: Too often, plans are developed and then put aside until they are needed. Like any aspect of a business, the assumptions that go into a crisis communication plan need to be reviewed and updated. People, organizations, conditions, and technology all undergo modification and change. Intuition tells us that any plan that isn't periodically reviewed and updated will gradually lose its relevancy. Given the important life-safety nature of the crisis communication plan an annual review is the minimum review cycle recommended by The Resiliency Institute.

Selected Response: No

Recommendation: The assumptions that surround a review of the crisis communication plan should be periodically modified to stress different aspects of the plan. If you don't have a plan, then clearly you can't review it. Alternatively, if you have a plan and don't review the information contained in it, especially contact information, then it runs the risk of becoming obsolete and more of a hindrance than an aid in a crisis. A simple example of what is meant by changing a planning assumption is to review the different procedures followed in a shelter-in-place versus evacuation scenario. Another might have to do with notification of an important news event (a violent act at a school or shopping mall, outbreak of a new strain of flu, etc.), or something that affects the organization such as the announcement of a merger or the resignation of a key executive. These scenarios test different aspects of the crisis plan and its integration with the overall resiliency program. An annual review is a good practice, but more frequent reviews – especially of the contact information – is encouraged. Having gone to the trouble of creating a plan it is a good practice to maintain it.

Question #3: Is there an approved budget to support this portion of the overall preparedness plan?

General Comments: Crisis communication plans need not be a financial drain. Many aspects of the plan can be implemented with little or no cost. Call trees can be implemented inexpensively as can the preparation of material for possible distribution to the media. Of course, there are sophisticated notification systems on the market, but there are also many inexpensive things that can be done with the various cell phones that are in use. Nextel, RIM (maker of the Blackberry PDA), the iPhone, etc. – all have impressive notification capabilities. It doesn't take a lot of money to tap into the capabilities of these and other devices and integrate them into the crisis communications plan.

Selected Response: Unknown

Recommendation: Determining if the crisis communication plan is supported by a budget should not be a difficult task. The Resiliency Institute suggests that you determine the correct answer and then return to and modify your answers according. To change your response to a question, please send a request via email to: The Resiliency Institute@NorthRiverSolutions.com. A member of our The Resiliency Institute™ team will provide you with instructions on how to modify your response. This will lead to an automatic recalculation of your index score

Question #4: Has a specific individual been given responsibility for the firm's crisis communication plan?

General Comments: As in the case of any other portion of the resiliency plan, having an individual assigned to manage and direct this segment helps to bring focus to the effort.

Selected Response: Partially

Recommendation: Once this portion of the resiliency program is established, it is important to designate leaders (always designate at least one backup!) who are trained and prepared to deal with the media. The Resiliency Institute recommends having them go through a program of media training. Such courses are available online and onsite. For more information contact The Resiliency Institute.

Section 3: Facilities and Security Management

(There are 60 questions in this section. Below are a representative sample of the questions.)

Question #7: Does the firm have a plan to move to an alternative site in the event of an emergency that damaged the primary facility?

General Comments: The need for an alternative work site may arise from even a minor disruption. Your building may be closed due to a large community event for several days. This happens every four years to those working near our nation’s capital during presidential inaugurations. Planning for this alternate worksite is more than finding a facility of adequate square foot capacity. It includes all aspects of support for all relocated business functions. Infrequently used equipment such as secure facsimile machines or specialized printers may be forgotten but are vital to the full functioning of the moved processes.

Selected Response: No

Recommendation: You should determine whether an alternate facility is needed and how you can manage the move and recovery at this new site. This response may also indicate that a full and thorough plan has not been developed. All organizations should prepare to temporarily operate at an alternate location. If the site is not provisioned or capable of being provisioned on short notice in a manner adequate to support your operations, it may be essentially useless. Give a very high priority to determining the functions which will be relocated and insure that the alternate site can fully support the most critical functions in all aspects.

Question #8: Do employees sign non-disclosure and confidentiality agreements?

General Comments: Organizations need to ensure that as part of their overall planning to continue operations, both physical and intellectual assets are protected. Each organization has valuable proprietary and private information which should not be published. Examples of two important documents are the business continuity and disaster recovery plans. These should be shared with appropriate individuals, but unless carefully crafted could, at least in theory, supply information to those who would harm the organization with areas of vulnerability and weakness. Like any other business plan, DR and BC plans should not be shared and it is good practice to have employees sign non-disclosure agreements and to identify these plans as company confidential.

Selected Response: No

Recommendation: Not having this procedure in place is of concern to The Resiliency Institute analysts. This procedure is viewed as both a good business practice and a sign of the organization's attention to basic self-protection. This area is clearly impacted by the need to share information with public safety agencies. It is suggested that you implement some type of document tracking and version control to monitor the completeness of this program. Ensuring that private or confidential information is not released is vitally important. These same procedures will help ensure that employees know the importance of not speaking about certain issues. The Resiliency Institute suggests you discuss this issue with your corporate attorney to gain a complete understanding of this important issue.

Question #9: Has a specific individual been given responsibility for the firm's facilities?

General Comments: Having an individual assigned responsibility for managing and maintaining this portion of the business resiliency plan is a best practice. For some single site operations dependent on the availability of an outside alternate work site during a disruption, this is a critical path issue. For others with multiple locations performing similar or identical functions, this role takes on less importance.

Selected Response: Yes

Recommendation: Since you have assigned one or more individuals this role, The Resiliency Institute suggests encouraging them to join one of the national organizations that deal with facility issues. There are specialized training programs available and even useful certifications. Consult the Resource Center for more information on these programs.

Question #10: Is there an on-site security presence?

General Comments: Many facilities are leased and shared by two or more organizations and managed by a professional firm. This may lead to very effective security procedures, but also means that the procedures may not be subject to approval and review by your organization. For example, they may or may not provide on-site security personnel. If they do, often these individuals are primarily found in the lobby. Security beyond this level may seem extravagant, but it should be considered. An example of a heighten need for security would

arise if there was a restraining order issued on behalf of the company or any employee. Such an action could lead to an increased security threat. It is important to track the community and take note of any increase in local crime. A new tenant in a shared facility might increase the security or risk. For example, a bank, high security firms such as military contractors, or certain types of medical operations could all indicate a need for additional on-site security. This resource does not have to be dedicated and is often shared by the entire facility.

Selected Response: Yes

Recommendation: Considering your answer, our analysts wonder if these individuals are employees or contractors of your organization or supplied by the property managers? If these are employees, then the plan should specify the type and frequency of background checks made before a job is offered. If these individuals are provided through a service, then these same issues should be addressed in the contract between the parties. In any case, having onsite security helps reduce the threat level from many risks. Even a token security presence is an important deterrent.

Question #11: Are security personnel trained to handle onsite violence?

General Comments: The nature of your facility and the environment will determine the level of security required. Theft, assault, corporate espionage, unauthorized systems access, terrorism, hurricanes and tornadoes, sabotage, vandalism, fire, explosions, and other threats, should be evaluated as you seek ways to meet security needs. Whatever type of security strategy you employ; outsourced services, in-house security, or reception staff supervising facility access; it is good business to provide training in handling violent behavior. The training can be as simple as understanding how to identify indicators, properly documenting a threatening phone call, or learning how to prevent violence.

Selected Response: Yes

Remaining Sections of this Report

Section 4: Operational Infrastructure: (There are 25 questions in this section)
Section 5: Technical Infrastructure: (There are 52 questions in this section)
Section 6: Human Resource Management: (There are 25 questions in this section)
Section 7: Continuity Management: (There are 26 questions in this section)
Section 8: Financial Control: (There are 14 questions in this section)
Section 9: Governance and Compliance: (There are 25 questions in this section)
Section 10: External Business Chains: (There are 21 questions in this section)
Section 11: Community and Environmental Stewardship: (There are 19 questions in this section)
Section 12: Risk Management and Control: (There are 20 questions in this section)

Closing Comments

We hope you find this information useful for further discussion and meaningful to your planning and understanding of the current state of readiness.

The Resiliency Institute, LLC., SAMPLE COMPANY, and your local insurance agency.

The comments made in this document are intended as discussion points for consideration and further investigation and are not recommendations. The Resiliency Institute does not certify nor represent that these discussion points are the correct or best possible response to the questions raised in this discussion. The Resiliency Institute disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, The Resiliency Institute is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is The Resiliency Institute undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

Appendix A: Business Continuity Glossary

(Omitted in this sample report)

Appendix B: Flood Plain Data

Image of FEMA Flood Plain Map