# Business Continuity Planning

## H & H Graphics, Inc.

Company Wide

Date February 2, 2016

# Contents

## Purpose

Use this process to create, maintain and review the company business continuity plan.

## Process Steps


This process is designed as a guide for identifying potential risks and analyzing probable risks in order to understand simple mitigations and high impact risks. Once areas are identified for mitigation, create a strategy for addressing each area; develop a plan that simply explains steps to be taken to prevent the risk and steps to be taken in the event the risk becomes reality. Finally, how to create test plans to confirm the plan will work before something actually happens and develop a way to keep the plan up-to-date.

Keep in mind that this is an iterative process that should be repeated on a regular basis in order to keep your plans current and to identify any new vulnerabilities and threats. Since change is a constant, your business continuity plan cannot afford to be.

## Identify

Before jumping into risk analysis, let's first learn some vocabulary.

**Threat** – Potential harm to personnel, finances, facilities, etc. that are outside of our control.

**Vulnerability** – Exposure to harm due to a weakness.

**Risk** – The probability of harm caused my external or internal threats and/or vulnerabilities.

In risk analysis, you identify threats and vulnerabilities that have the potential of negatively impacting the company. Then you assign risk to each of those – how likely is each to occur? Using the following risk matrix can be helpful.

| | | A | B | C | D | E |
|---|---|---|---|---|---|---|
| | | Negligible | Minor | Moderate | Significant | Severe |
| E | Very Likely | Low Med | Medium | Med Hi | High | High |
| D | Likely | Low | Low Med | Medium | Med Hi | High |
| C | Possible | Low | Low Med | Medium | Med Hi | Med Hi |
| B | Unlikely | Low | Low Med | Low Med | Medium | Med Hi |
| A | Very Unlikely | Low | Low | Low Med | Medium | Medium |

Consider each threat and vulnerability based on its likeliness to happen AND the overall impact. Those items in red are the ones you work first.

## Analyze

Once you identify the threats and vulnerabilities to focus on, take the impact analysis to the next level. Below is an example of impact analysis.

**[Company Name]**
**Risk Assessment and Financial Impact Model**
**[Date]**

Gray cells are calculated for you. You do not need to enter anything into them.

| Risk area | Potential risk | Number of annual incidents | Cost per incident | Total annual cost | Probability of occurrence | Weighted cost | Mitigati |
|---|---|---|---|---|---|---|---|
| Competitive | Contoso, Ltd. might introduce a superior offering on June 30 to compete with our #1 product line. | 1.00 | $1,850,000 | $1,850,000 | 75.0% | $1,387,500 | Reduce pric the volume s |
| | | | | $0 | | $0 | |
| Economic/political | | | | $0 | | $0 | |
| | | | | $0 | | $0 | |
| Regulatory/legal | Need to meet Sarbanes-Oxley 404 (SOX) compliance requirements by target date. | 1.00 | $15,000,000 | $15,000,000 | 5.0% | $750,000 | Establish SO January 15 t before requir |
| | | | | $0 | | $0 | |
| | | | | $0 | | $0 | |
| Technological | Potential exists for hackers to compromise internal network and obtain | 5.00 | $4,000,000 | $20,000,000 | 10.0% | $2,000,000 | Upgrade firev proxy server |

Risk Assessment Scorecard | Sample 1—Competitive Risk | Sample 2—Operational Risk

You can use this analysis to dig further into the vulnerability/threat to identify specific impact areas. Where are the costs highest? What things are easily mitigated? What areas have such a negative impact that they cannot be ignored?

## Design

In design, develop mitigations that reduce the likelihood of a vulnerability/threat, eliminate it all together or provide a method for reducing the impact when it becomes a reality. This step will require assistance from the impacted team members.

## Execution

Execution includes several things. First, taking action to change situations, processes, etc. in order to eliminate or reduce the risk of a vulnerability/threat. Execution is also documenting and educating staff on steps to take when disaster strikes.

## Measure

Measure is a critical step. This is testing actions taken and process developed to see if they are really effective. Many times we do not have a clear picture of everything that would be impacted in the event something bad happens – like all communication methods go down. By testing, those things are brought to light. By testing, you can also eliminate bad assumptions.

Once testing is complete, gather a team together to create lessons learned and use those to improve documented procedures.