Risk Assessment Practices

By: Wilfredo R. Vera Pujols
Dr. Nelliud Torres
Polytechnic University of PR

Abstract

To an enterprise, one of the most important assessment that should develop is the Risk Assessment. This practice includes identify the threats that can affect the business continuity. In addition, is necessary classify them to perform an analysis where we can identify the riskiest threats to the operation. This project establishes the importance of a Risk Assessment for an organization. Based on ISO 22301 [1], the new international standard for business continuity management systems is designed to specify the requirements for setting up and managing an effective Business Continuity Management System (BCMS) for any organization, regardless of type or size. To effectuate the assessment is fundamental create a methodology to assess the risks and threats. The result of the analysis should be discussed with the management and they need to determine what controls are cost effective to implement or if the organization can accept the risk. To perform the process of a Risk Assessment we select an organization of technology to determine the possible threats that should affect the facilities or the operation in different scenarios.

Objective

The objective of the Risk Assessment is to identify and evaluate the key threats that could cause an interruption in the operation of the enterprise. In addition, obtain as a result the residual risk of each determined threat.

Scope

A Risk Assessment should be performed in the appropriate ways to evaluate current and future risks for the facility and the business operation. We are going to analyze the risks based on the natural, man-made and technology threats that should affect the continuity of the operation. As a result, the Risk Assessment Report will illustrate the residual risk from where the organization are going to evaluate the impact of each threat and determine if they need to implement additional controls to mitigate the risk.

Methodology

To develop the Risk Assessment, we will use the survey process to gather the input of the responsible areas of the threats. Moreover, the process of interview is going to be to the different departments in the company such as: Human Resources, Physical Security, Information Security and Facilities.

Threat Assessment

Threat	Theat Description	Threat History
Earthquake	Any sudden shaking of the ground caused by the passage of seismic waves through Earth's rocks	The "Puerto Rico Trench," a 560 mile long under-ocean canyon and fault line, is one of the deepest in the world and b the British Virgin Islands, continued throughout the north of Puerto Rico and goes almost to the Bahamas. The deepe trench is close to the northern Arecibo. The seismic vulnerability study conducted by Dr. William McCann in 1987 yielded a probability of 33-50% of a stro different parts of the island for a period of 50 years. A 2003 study from the USGS revealed that West-Southwest Puer the most vulnerable to earthquakes. According with the "Red Sismica de Puerto Rico", the most significant earthquake occurred in the island were: 08/15/1670: Damages reported in San Germian and San Juan. 05/02/1787: Damages reported across the island, except south coast. San Juan reported several damage and various st collapsed. 11/18/1867: 7.3 of magnitude in Virgin Islands. Several damages were reported in Virgin Islands and Puerto Rico. 10/11/1918: The epicenter was located about 35 km northwest of Aguadilla. Their magnitude was 7.3. This earthquak tsunami that reached 20 feet in Punta Aguajera (8 people drowned), 12 feet in Aguadilla (32 people drowned) and 5 fe The earthquake killed 116 people. For several months, aftershocks of this earthquake were felt, the strongest on Octo November 12. 07/28/1943: Occur in North-West side of island. The magnitude of 7.5. No major damages occur. Mild to minor tremors have been felt almost every year without consequences nor damages.

Vulnerability	Control	Type of Risk
1) Geographical position - The Puerto Rico Trench is located at a boundary bet plates. The Caribbean Plate is moving to the east while the North American Pla moving to the west. "Puerto Rico Trench", one of deepest in the world. 2) Scientific studies have concluded that an earthquake occurring along this fa could generate a significant tsunami. The Puerto Rican Seismic Society has bee use the Puerto Rican media to inform people about a future earthquake that cou in a catastrophic tragedy.	1) The Main Building complies with the PR construction codes. Construction c have been developed to manage significant earthquake resistance.	Natural Threat

Dimensions Used to Asses Risk

The identified threats are going to be evaluated using the impact, likelihood and control metric. [5] To determine the risk score we calculate the rates of each metric and the result can determine the residual risk of the organization. The residual risk is the risk that remains after the controls were implemented. In other words, this result can provide the total risk necessary to avoid, accept or transfer it. It can be low, medium or high.

Metrics

Likelihood Metrics

Value	Likelihood	Scale	Description
1	Rare	≥5%	Minor exposure, minor severity.
2	Unlikely	6%–25%	Minor exposure, moderate severity; or moderate exposure, minor severity.
3	Occasional	26%–50%	Highly exposed, minor severity; or minor exposure, high severity; or moderate exposure, moderate severity.
4	Likely	51%–75%	Highly exposed, moderate severity; or, moderate exposure, high severity.
5	Almost Certain	76%–	Highly exposed, high severity.

Consequences Metrics

Qualitative or Quantitative				
Value	Consequences	Financial Loss	Standing Loss	Personal
1	Insignificant	Almost No Loss	Insignificant	Minimal to no impact of meeting key functional targets.
2	Minor	Insignificant Loss	Minor	Minor impact of meeting key functional targets.
3	Moderate	Notable Financial Loss	Moderate	Moderate impact on meeting key functional targets.
4	Major	Material Financial Loss	Major	Serious impact on meeting key functional targets.
5	Catastrophic	Threatens Financial Loss	Catastrophic	Several key employees or mass departmental departures.

Control Metrics

Rate	Mitigation Control	Effectiveness of Contro reducing inherent Ris	Control Determinated
1	No Control	0% Efective	Process is clearly deficient in critical ways.
2	Deficient	10% Effective	Process present some deficient in critical ways.
3	Adequate	25% Effective	Process present are acceptable.
4	Effective	50% Effective	Process are sufficients to minimize the risk.
5	Excessive	75% Effective	Process are excesive to mitigate the risk.

Recommendation

In the data communications, the recommendation is to add another service provider with different service entrance to mitigate the problem in case of a failure. Moreover, double the water reserve to had more available in case of prolonged drought. Furthermore, is recommended to increase the physical security in order to minimize the residual risk of bomb, explosion or terrorism threat. However, to mitigate the errors in the contracts the management should implement a process of vendor management, this process can validate every contract effectuated from a third party. Furthermore, the organization should coordinate with the department of Human Resources an emergency plan to orientate and explain the employees how to respond in case of an earthquake.

Risk Assessment Report

This Assessment (see Figure 6) presents the results of the all data collected. Based on the interviews and the threat assessment, we rate each threat based on our perspective on how the organization could be affected. Furthermore, it presents the result of residual risk based on Low, Medium or High criteria. It is important to explain that if the risk score is less than seven (7) the residual risk is Low. However, if is less or equal than thirteen (13) the risk score is Medium and if it is above thirteen (13) it will be considered High. Thus, the higher risk score and residual risk, the more controls and mitigation procedures must be implemented. Meanwhile, the management of the organization could understand that the result of the threat does not affect in a big scale its business continuity.

Risk Assessment						
Threat	Impact	Likelihood	Control	Risk Score	Residual Risk	Responsible
Natural Threats						
Earthquake	5	3	3	11.25	MEDIUM	Physical Security
Epidemics / Pandemics	4	2	3	6	LOW	Human Resources
Flood / Water	2	3	3	4.5	LOW	Facilities
Hail	3	3	2	8.1	MEDIUM	Facilities
Hurricane / Storm Surge	5	5	4	12.5	MEDIUM	Facilities / Human Resources
Landslide / Mudslide	2	1	1	2	LOW	Facilities
Thunderstorm / Lightning	3	1	4	1.5	LOW	Facilities
Tornado / High Winds	3	1	2	2.7	LOW	Facilities
Tsunami	1	1	4	0.5	LOW	Facilities / Human Resources
Drought	3	4	2	10.8	MEDIUM	Facilities
Man-Made Threats						
Acts of Terrorism / Sabotage / Vandalism / Riots	5	2	2	9	MEDIUM	Physical Security
Bombs Threat	5	2	2	9	MEDIUM	Physical Security
Contamination / Hazmat Event	2	1	2	1.8	LOW	Facilities / Physical Security
Contractor errors	4	2	2	7.2	MEDIUM	Information Security
Disgruntled Employees	3	3	2	8.1	MEDIUM	Human Resources
Explosion	5	2	2	9	MEDIUM	Facilities / Physical Security
Fire	5	2	2	9	MEDIUM	Facilities
Transportation	1	1	1	1	LOW	Physical Security
Flood (Burst-Pipe)	3	2	4	3	LOW	Facilities
Power Outage	5	3	4	7.5	MEDIUM	Facilities
Technology / Infrastructure Threats						
Data Communications Failure	4	3	3	9	MEDIUM	Information Security
Voice Communications Failure	3	2	3	4.5	LOW	Information Security
Power Failures	4	2	4	4	LOW	Facilities
Distributed Denial-of-Service (DDoS) attack	5	5	4	12.5	MEDIUM	Information Security
Ramsomware	5	2	4	5	LOW	Information Security
Data Breach	4	2	4	4	LOW	Information Security
Hardware Failure	4	5	4	10	MEDIUM	Information Security
Software Failure	4	5	4	10	MEDIUM	Information Security

Conclusion

During the analysis of the results, we understand the control environment that the organization had to ensure the business continuity. Later of analyzing the results of the Risk Assessment as a deliverable, the conclusion is that the organization should implement more controls to minimize the residual risk. In summary, the organization accept the results and identified the importance of mitigate those risks. The implementation of new controls is going to be discussed with the management and they will determined the necessity of them according the priority of the organization. Otherwise, they need to accept the mentioned risks and implement plans to mitigate those threats. However, any changes in the actual controls of the organization needs to be notified to update this report.

References

[1] *ISO 22301*. International Standard, Switzerland. 2012.
[2] (2018, 05, 01) *ISO 22301, Implementation Guide.* Business Continuity Group. Available: https://www.bsigroup.com/.(https://www.bsigroup.com/globalassets/Documents/iso-22301/resources/iso-22301 -implementation-guide-2016.pdf).
[3] *Red Sismica de Puerto Rico*. (2018, 05 01). Retrieved from Red Sismica de Puerto Rico: Available: http://redsismica.uprm.edu. (http://redsismica.uprm.edu).
[4] Frigo, M. L., & Anderson, R. J., "Strategic Risk Assessment", Strategic Finance, Institute of Management Accountants, Inc., N.J., December 2009, pp. 25-33.
[5] Hancock, B. V. 2015. *Survey of Risk Assessment Practices*. Available: https://erm.ncsu.edu/. (https://erm.ncsu.edu/az/erm/i/chan/library/Risk_Assessment_Practices_Thought_Paper_ERM_NCSTATE_2015.pdf).
[6] (2018, 06, 2018) *Hurricane Maria.* Available: https://edition.cnn.com/ (https://edition.cnn.com/specials/weather/hurricane-maria).