Risk Assessment Practices

Wilfredo R Vera Pujols
Master in Computer Science
Advisor: Prof. Nelliud Torres, DBA
Electrical and Computer Engineering & Computer Science Department
Polytechnic University of Puerto Rico

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. 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.*

Key Terms – *Assessment, Business Continuity, ISO 22301, Risk, Threat.*

INTRODUCTION

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. The institution of British Standards recommends that every business has a system in place to avoid excessive downtime and reduced productivity in the event of an interruption. ISO 22301 was designed to be used by internal and external parties to assess the organization's ability to meet regulatory and customer requirements as well as the organization's own requirements. The organization can use this document to follow the practice guidance and recommendations, indicating which practices should, or may, undertake to implement effective Business Continuity Management (BCM). Furthermore, ISO 22301 [1] only establish those requirements that can be objectively audited and represent the best way of implementation that an organization can used to assure interested parties maintain an appropriate Business Continuity Management Standards. In addition, can be used to assess its suppliers' ability to meet business continuity needs and obligations.

Moreover, the way that the ISO 22301 [1] indicate what practices an organization should, or may, undertake to implement effective BCM are represent into ten clauses (see Figure 1). The standard establishes on the Clause 8.2.3 [1] the Risk Assessment as a process to develop and manage the risks of the BCMS correctly. This Clause indicates, "draws attention to the fact that 'certain financial or governmental obligations require the communication'. In addition, explains "at varying levels of detail, of the risks that could disrupt the prioritized activities." [1].

However, is important to define correctly the word risk because that could help to identify and analyze the possible threats in which the organization can be vulnerable. The way that every organization can develop this process are going to be aligned to the specific needs and culture of the organization [2]. The Risk Assessment is the process of identify, analyze and evaluate the nature and impact of vulnerabilities, risks and opportunities that can result due to the lack of appropriate controls or effects of potential events.

In other hand, 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. This organization is focused in the develop and manufacture technology industry. They identify that the risk of an interruption in their site may affect the profit or even the loss of the primary clients. In that instance, the organization determine to perform a Risk Assessment based on the ISO 22301 to evaluate the threats to which they are exposed versus the controls implemented. We are going to identify in

this project the possible threats based on the location, the operation and every possible event on which they could be exposed or affected. This project is based in the data provided by an anonymous company with the main Data Center located at San Juan, Puerto Rico. As consequence, and for confidential purpose not more information about the company would be provided.

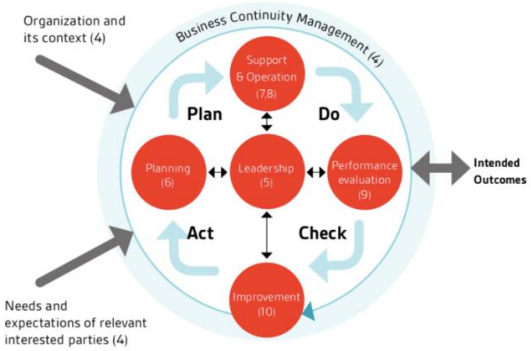

Figure 1
Business Continuity Management Diagram [3] (Illustrates the interaction of the different clauses determined by ISO 22301)

RISK ASSESSMENT

The Risk Assessment (RA) is the process of identify, analyze and evaluate the nature and impact of vulnerabilities, risks and opportunities that can result due to the lack of appropriate controls or effects of potential events. To perform a complete Risk Assessment, we need to execute some basic considerations to develop the process of assessing the risks;

- Identify the most probable threats or risks that may cause a business interruption.
- Identify Responsible of these threats.
- Create the Assessment Methodology.
- Choose the dimensions to evaluate:
  - Likelihood
  - Consequences
  - Control
- Choose the scale to evaluate the Assessment:
  - 3 points
  - 5 points
- Choose the dimension to evaluate the Assessment:
  - Surveys
  - Interviews
  - Workshops
- Develop the formula to obtain results
  - Consequence * Likelihood * Percentage of Control (%).
- Analyze the probability of occurrence for those threats.
- Identify the consequence of occurrence of any of the identified threats.
- Identify controls that mitigate or reduce the level of risk associated with the threat.
- Understand the residual risks for the identified threats:
  - Low
  - Medium
  - High
- Request implementation of mitigation plans, if required, or accept the residual risks.
- Report.

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.

COMPONENTS

The threats to be identified in the Risk Assessment are being classified into:

- Natural Threat
- Man-Made Threat
- Technology Threat

THREATS

Based on the location and the culture of the organization there is the list of the threats identified (see Figure 2).

Threat Type and Description		
Natural Threats	Man-Made Threats	Technology / Infrastructure Threats
Earthquake	Acts of Terrorism / Sabotage / Vandalism / Riots	Data Communications failure
Epidemics/Pandemic	Bombs threat	Voice Communications failure
Flood / Water	Contamination / Hazmat Event	Power Failures
Hail	Contractor errors	Distributed denial-of-service (DDoS) attack
Hurricane / Storm Surge	Disgruntled employees	Ransomware
Landslide / Mudslide	Explosion	Data breach
Thunderstorm / Lightning	Fire	Hardware Failure
Tornado / High Winds	Transportation	Software Failure
Tsunami	Flood (Burst-Pipe)	
Drought	Power Outage	

Figure 2
List of the Different Types and Description of Possible Threats such as: Natural, Man-Made and Technology/Infrastructure

DELIVERABLES

A Risk Assessment Report that provides the risk score of the different threats determined by the analysis. Furthermore, the Risk Assessment will present the level of the Residual Risk that the organization need to accept or to mitigate of each particular threat.

ROLES AND RESPONSIBILITIES

The Business Continuity Unit (BCU) is responsible for performing the Risk Assessment, developing the report, and informing the results to the high management.

FREQUENCY

The Risk Assessment process should be reviewed and updated at least once a year. The recommendation is to update the Assessment if occurs a radically change on a facility that may change the result of the analysis.

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.

Dimensions Used to Assess Risk

The identified threats are going to be evaluated using the impact, likelihood and control metric [4]. 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 to Assess Risk

To evaluate the threats identified in the analysis we will rated in three different metrics. These metrics represent the level of rates to evaluate the likelihood, consequences and control implemented to obtain a result in the Risk Assessment Report. The formula to calculate the residual risk is = Consequence * Likelihood * The percentage of effectiveness of the control implemented. In the scale, five points is the high level of rate and one point is the lowest.

Likelihood Metric

The Likelihood Metric (see Figure 3) evaluates the likelihood between one to five. The number one rate represent how rare is the event to occur based on history. Nevertheless, number five represent the highest rate and the most probable event to occur. The Threat Assessment shows the threat history related to the location of the organization.

Consequences Metric

The Consequences Metric (see Figure 4) evaluates the consequences on qualitative or

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.

Figure 3

Likelihood Metric (It is used to evaluate the likelihood of the event to occur)

quantitative ways that the threat may affect. The metric is classified in Consequences and different losses such as: Financial, Standing and Personal. Financial loss evaluates the monetary consequence using a range of the money loss. Standing loss is related to the consequences that can affect the public. Personal loss represents the rate of personal that may quit to the job or start to be absent and are not performing their duties. Since risks are difficult to quantify, we are going to determine the rate according to the interview.

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.

Figure 4

Consequences Metric (Describes the qualitative or quantitative consequences that can affect the organization)

Control Metric

The Control Metric (see Figure 5) represent the rates to evaluate the percentage of control that the organization has implemented. As an example, if the organization we understand that the control is deficient, we select the rate 2. Then, in the formula to calculate the residual risk we will use the percentage of the rate 25% to obtain the result.

THREAT ASSESSMENT

The Threat Assessment presents multiple segments which describe the risk and relevant threats identified by the organization. The description segment of the assessment includes a brief description and relevant information of the threats. Otherwise, history summarizes multiple events related to these threats or near the location of the organization. Finally, the vulnerability segment establishes different risks identified by the organization related to the mentioned threats. In order to obtain the assessments' results, I performed a research using multiple reliable web sources including but not limited to; http://redsismica.uprm.edu [5], https://edition.cnn.com/ [6].

Rate	Mitigation Control	Effectiveness of Control reducing Inherent Risk	Control Determinated
1	No Control	0% Effective	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.

Figure 5

Control Metric (Describes the control in percentage of effectiveness)

Additionally, I interviewed different sources with knowledge and expertise in these topics to add additional assurance. The rates and results included on the metric below are rely directly on this assessment.

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

Figure 6

Risk Assessment Report with the Results after the Analysis of the Threats from the Organization

RECOMMENDATIONS

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.

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] International Organization of Standardization, *ISO 22301*, 2012.

[2] M. L. Frigo & R. J. Anderson. (2009, Dec 1). *Strategic Risk Assessment* [Online]. Available FTP: https://www.rims.org Directory: resources/ERM/Documents File: StrategicRisk Assessment_StrategicFinance_December2009.pdf.

[3] BSI Group. (2018, May 01). *ISO 22301, Implementation Guide* [Online]. Available: https://www.bsigroup.com/globalassets/Documents/iso-22301/resources/iso-22301-implementation-guide-2016.pdf.

[4] B. V. Hancock. (2015). *Survey of Risk Assessment Practices* [Online]. Available FTP: https://erm.ncsu.edu/az/erm/i/chan/library/Risk_Assessment_Practices_Thought_Paper_ERM_NCSTATE_2015.pdf.

[5] UPR – Mayagüez. (2018, May 01). *Red Sismica de Puerto Rico* [Online]. Available: http://redsismica.uprm.edu.

[6] CNN. (2018, Nov. 06). *Hurricane Maria* [Online]. Available: https://edition.cnn.com/specials/weather/hurricane-maria.