Trust in the cloud by viewing risk holistically: A Web-Based Risk Analysis Tool using FRAAP for SAP HEC and a Cloud Provider

Daniel de Jager

Academy for Computer Science and Software Engineering,
University of Johannesburg,
South Africa,
DanielDeJ@Discovery.co.za

Abstract. Cloud Providers are at times unaware of the risks brought into the cloud by their clients. They might be hosting software on the cloud that was not subject to rigorous Information Assurance practice as a result of lacking information security governance maturity. In most cases, cloud providers contractually bind clients with agreements in order to prevent risks to be realised on the upper layers of the cloud stack. However, without data collection points and analysis of the risks on both sides of the coin, there will not be a consolidated view of risks. This paper presents an online web-based risk analysis tool in order to provide a holistic view of risks "above" the cloud and "below" the cloud. The inspiration for this tool came about from SAP HANA Enterprise Cloud being implemented on the Cloud locally in South-Africa and discussions with Cloud Provider Risk Managers based in Ashburn, Virginia. The software was written with the Facilitated Risk Analysis and Assessment Process in mind. The input to the tool follows a facilitated process of risk identification and control selection. The software then can calculates the Risk Rating for each identified risk and is able to visually articulate the business attributes based on integrity, availability and confidentiality, as well as above and below the cloud, and lastly provide a holistic calculation of the entire stack i.e. per instance quantitavely and for all SAP Sites qualitatively.

Keywords: Risk Analysis, Facilitated Risk Analysis and Assessment Process, Software-as-a-Service, Cloud-Computing, Web-Based Risk Analysis Tool

1. Introduction

The tool, known as Periculum, Latin term for Risk, attempts to provide a holistic view of risks for both Cloud Provider (CP) and Cloud Adopter (CA), and is based on multiple instances of SAP HANA Enterprise Cloud (SAP HEC).

The chosen risk assessment methodology is the Facilitated Risk Analysis and Assessment Process (FRAAP) which requires that a facilitator is used during the process in order to ensure that the risk analysis is done in line with business context (Peltier, 2005). The facilitator is regarded as an expert in the discipline of risk management since their decisions, views and experience can produce valued information, especially in the case of the uncertainty of what clients are installing in the cloud and the resulting consequences from a risk point of view (Clemen, 1999).

In Section 2, we propose a model for the risk analysis for SAP, taking into considerations the different paradigms of risk i.e. above the cloud, below the cloud, assessment domains and the three business attributes, Confidentiality, Integrity and Availability. Section 2 also shows the coding used to calculate two metrics, the Overall Score, which includes all SAP Sites and provides a qualitative measurement, and a overall quantitative score for an instance of a SAP Site.

Section 3 explains the Entity Relationship Model that is representative of the model presented in Section 2 and highlights the key tables and what their purpose is.

Section 4 shows the Risk Analysis process on the front end that has been developed for the tool. Implemented in JSF, and takes the reader though each phase and each step of the risk analysis process.

Section 5 provides the visuals provided by tool to articulate the two metrics. Section 6 is a critical evaluation of the implementation of the SAP Site concept.

This paper is then concluded in Section 6.

2. The Model for SAP HEC

2.1 The Model

The analysis and assessment is based on seven pre-defined domains, each having a sub-domain related to the business attributes of Confidentiality, Integrity and Availability. The seven domains are further split into two perspectives, namely above the cloud, and below the cloud. Above the cloud is the Cloud Stack for which the Cloud Adopter (client) is responsible for, and below the cloud, is the cloud stack for which the Cloud Provider is responsible for.

The seven domains are:

1. Problem Management
2. Security Incident Management
3. Change Management
4. Data Protection Regulations
5. Policy Management
6. Client Contract Management
7. Business Continuity Management

The three dimensions of the SAP Model is represented in Figure 1.

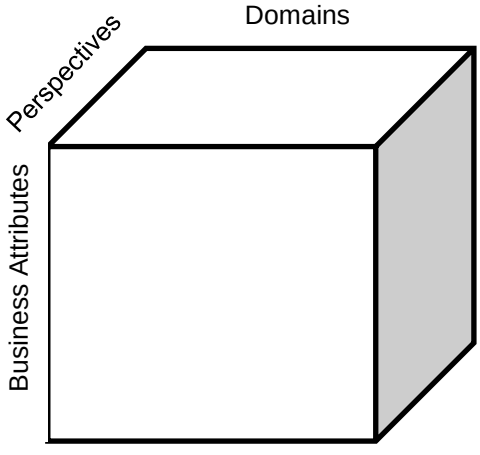

Figure 1 SAP Site Model

The Risk Analysis process then assesses each point in the model showed above.

2.2 Risk Rating Matrix

The Risk Rating Matrix is kept very simple, only taking into account the values for impact and probability for Low, Medium and High. The tool has the risk rating matrix built into the database as key value pairs. When the facilitator selects the impact and probability, the tool will perform a lookup in the database to find the impact and probability pair. The same record will contain the risk rating being either red, yellow or green.

Probability

Impact	Low	Medium	High
High			
Medium			
Low			

Table 1 Risk Rating Matrix

2.2 Risk Calculations

In total there are two metrics. In the following section we show the pseudocode for each. Risk calculations are performed on two levels. The first level is an overall view across all the SAP Sites and the second is on a per SAP Site basis per domain score using a quantitative method.

2.2.1 Metric 1: Overall Qualitative Score

Metric 1 merely adds the red, yellow and green findings for each item of risk in the risk register. Based on the count of red, yellow and green the tool will decide what the qualitative score is, being either High, Medium or Low.

```
For each Risk Item in RiskRegister
        Count confidentiality risks
        Count integrity risks
        Count availability risks

        Count Red Risks
        Count Yellow Risks
        Count Green Risks
End For

If red risks > yellow risks AND red risks > green risks
then Rating = High

If red risks = yellow risks AND red risks > green risks
then Rating = High

If red risks < yellow risks AND red risks >= green risks
then Rating = Medium
```

```
if red risks < yellow risks AND red risks < green risks
then Rating = Medium

if green risks > red risks AND green risks > yellow risks
then Rating = Low

if green risks > red risks AND green risks <= yellow risks
then Rating = Medium

if yellow risks > red risks AND yellow risks > green risks
then Rating = Medium
```

Figure 2 Pseudocode for Overall Qualitative Calculation

2.2.2 Metric 2: Per SAP Site per Domain Score

The final metric is to attempt to quantify the SAP Site instance as a total score out of 100. The Higher the score, the higher the risk and the lower the score the lower the risk in principle. The following pseudocode shows how the weights are used to calculate the score per domain and then to calculate the final score for the SAP Site.

```
User Selects the SAP Site to measure
System retrieves the SAPSite risk register data as register
System retrieves the SAP Site Assessment Criteria to use the pre-defined weights

Incident Weight = System.getWeight(i)
Problem Weight = System.getWeight(p)
Change Weight = System.getWeight(c)
Legal Weight = System.getWeight (l)
Contract Weight = System.getWeight (con)
Policy Weight = System.getWeight (pol)
Business Continuity Weight = System.getWeight (bcm)

For each risk item in risk register
  Calculate Total Records
  Count incident management records
  Count problem management records
  Count change management records
  Count bcm management records
  Count policy management records
  Count contract management records
End For

Score Incidents = Count Incidents * Weight Incidents
Score Problem = Count Problem * Weight Problem
Score Change = Count Change * Weight Change
Score Policy = Count Policy * Weight Policy
Score Contact = Count Contract * Weight Contract
Score BCM = Count BCM * Weight BCM

Calculate the total weight //which must be 100

FinalScore = Total Score per domain * Total Weight
```

Figure 3 Pseudocode for quantitative measurement

3. Entity Relationship Diagram

3.1 Core Tables

The core of the database is the RiskRegister, Assessment and SAPSite tables, each being populated by related tables.

A SAPSite is a logical entity consisting of a Client and a Data Center. In the implementation we only allow a client to have a single instance of SAP HEC and not multiple instances in the same data center. There is then a one-to-one relationship between SAPSite, Client and Data Center respectively. If a client needs a secondary SAP Site, then a different data center must be utilised.

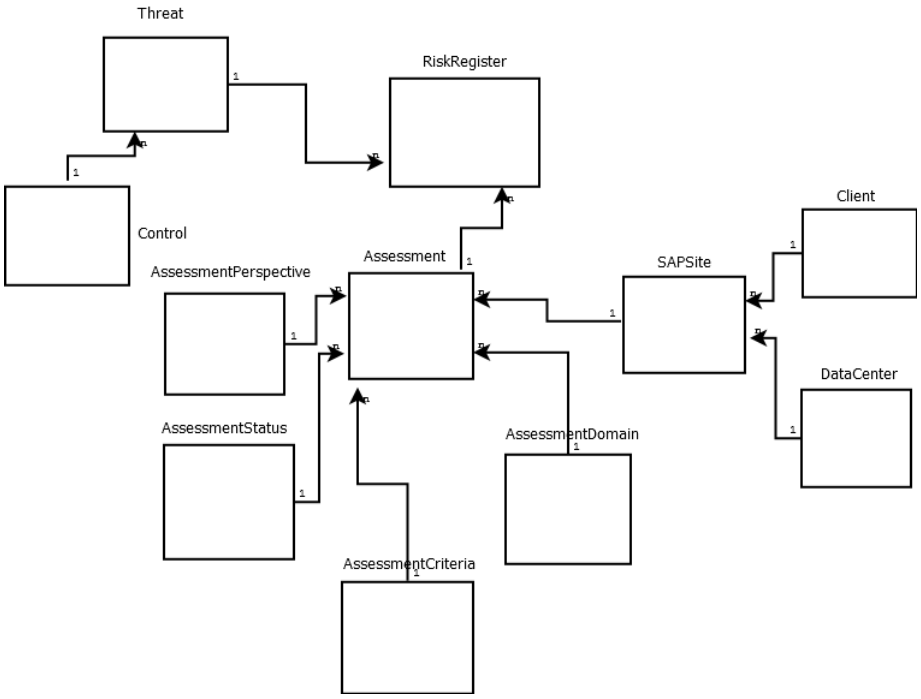

Figure 4 Periculum ER Diagram

3.2 Important Tables and Description

The most important tables for the risk assessment process is as follows:

Table Name	Function
Assessment	Stores data about an assessment, its start date, the SAP Site in scope, the facilitator and the status of the assessment.
AssessmentStatus	An assessment status is an enumeration of “new”,”initial”,”started”,”in progress” and “completed” and is an indication of where in the assessment process the facilitator is.
AssessmentCriteria	Stores weighting information relating to seven domains. The sum of all weights must equal 100.

AssessmentPerspective	The assessment perspective table stores static information regarding the viewpoint of risks, being either above the cloud or below the cloud
AssessmentDomain	There are seven assessment domains, each domain is stored in this table.
RiskRegister	The RiskRegister table stores risks for each assessment, risk items and their associated threats, controls, compensating controls, perspective, business attributes, impact and probabilities as well as the assessment domain.
Threat	A table storing the threat referred to in the RiskRegister,
Control	A table storing the controls identified during the FRAAP process.
RiskRating	A mapped out risk rating table exists to automatically calculate the risk rating of impact and probability values. A Risk rating can either be red, yellow or green.
BusinessAttribute	A Table storing the key value pairs for Confidentiality, Integrity and Availability.
DataCenter	A list of datacenters that the cloud provider uses for SAP HEC.
Client	A Client is a user of SAP HEC
SAPSite	A SAP Site is an instance of a client and a data center.

Table 2 Important Tables and Description

4. Java Server Faces (JSF) Implementation

The assessment is split into four phases. Phase 1 is concerned about the weightings per domain. Each domain is assigned a number between 0 and 100. The total weight for each of the seven domains must sum to 100. This gives the facilitator the ability to deem certain domains more important than other domains. Phase 2 is concerned about threat identification per SAP Site and Domain, Phase 3 is control selection and Phase 4 is to close out an assessment.

In the following sections we showcase the different phases.

3.1 Phase 1: Assessment Start and Weighting Allocation

The user is asked which SAP Site is in scope for the next assessment. The system then requires the facilitator to set weightings per domain. These values must range between 0 and 100, and the total weight for the assessment must sum to 100.

These weightings will be stored in the AssessmentCriteria table and will be used to calculate the overall score, which is a quantitative measurement of risk for a single instance of a SAP Site. The weighting input is shown in figure 5 below.

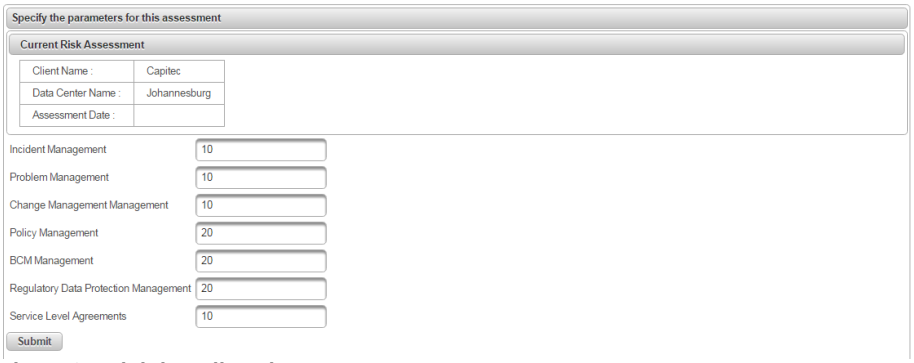

Figure 2 Weighting Allocation

3.2 Phase 2: Threat Identification

Step 1: Select the SAP Site, the perspective and the domain being assessed.

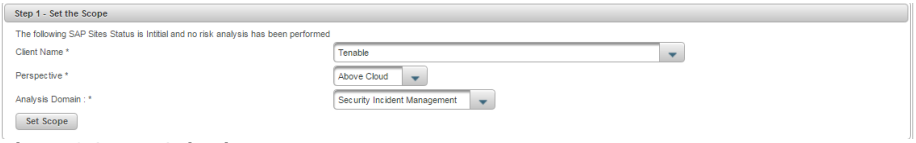

Figure 3 Scope Selection

Step 2: Within the Scope, perform threat identification. Only one threat can be identified at a time. If multiple threats exists, the entire process must be repeated.

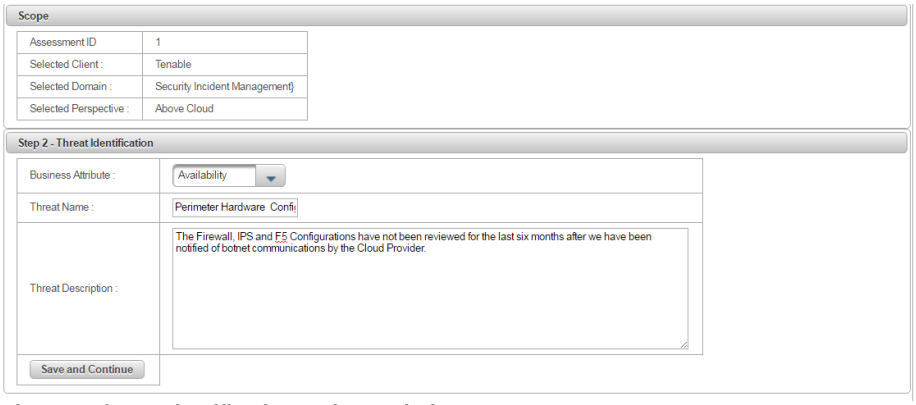

Figure 4 Threat Identification and Description

Step 3: Once the threat has been identified, the team including the facilitator indicates what the impact and probability of a realised risk event would be.

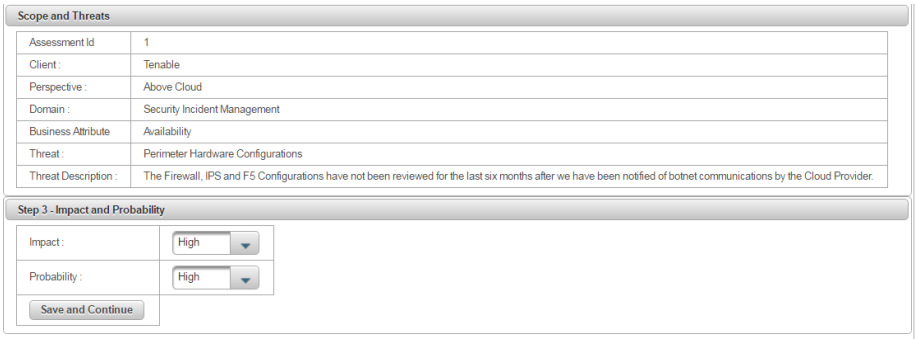

Figure 5 Impact and Probability Determination

Step 4: The tool will automatically calculate the Risk Level based on the matrix presented in section 2.2 The team and facilitator must indicate if the risk is acceptable or not.

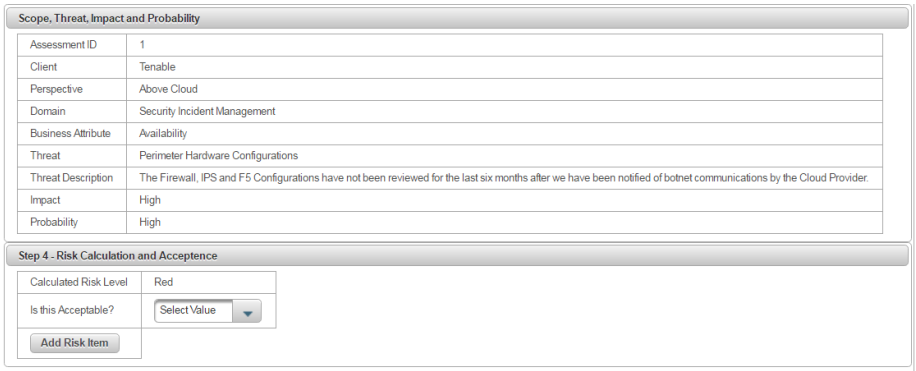

Figure 6 Automatic Risk Calculation and Acceptable Level Indication

3.3 Phase 3: Control Selection

The Control Selection Phase presents the facilitator with assessments that are in the started and in progress states.

Step1: Select SAP Site

Figure 7 SAP Site Selection

The SAP Site for the client Tenable in this example, is in the started phase since threats has been added to the assessment. Multiple threats exists in this example as can be seen in Figure x below.

Step 2: Select a threat in order to add a control.

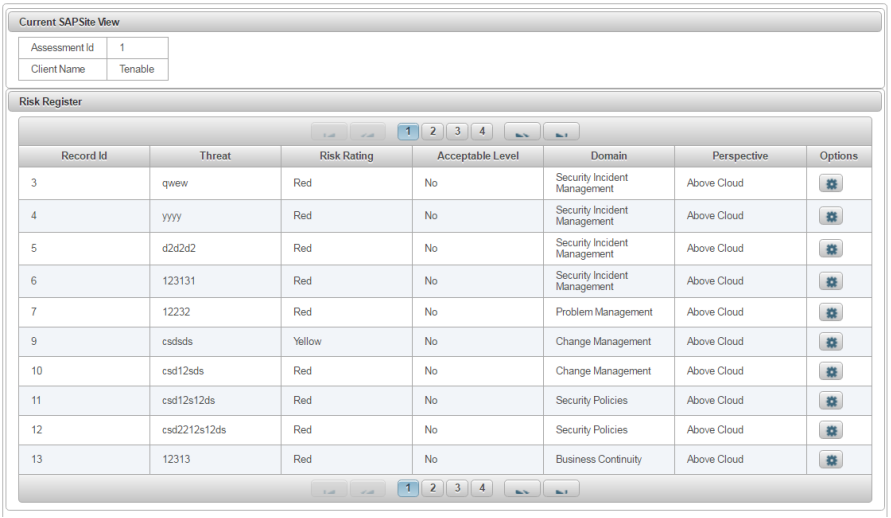

Figure 8 select a threat from a list of threats

Step 3: Populate the control fields. Indicate if the risk will be reduced and to what level by selecting a new impact and probability value. The tool will automatically calculate the risk rating.

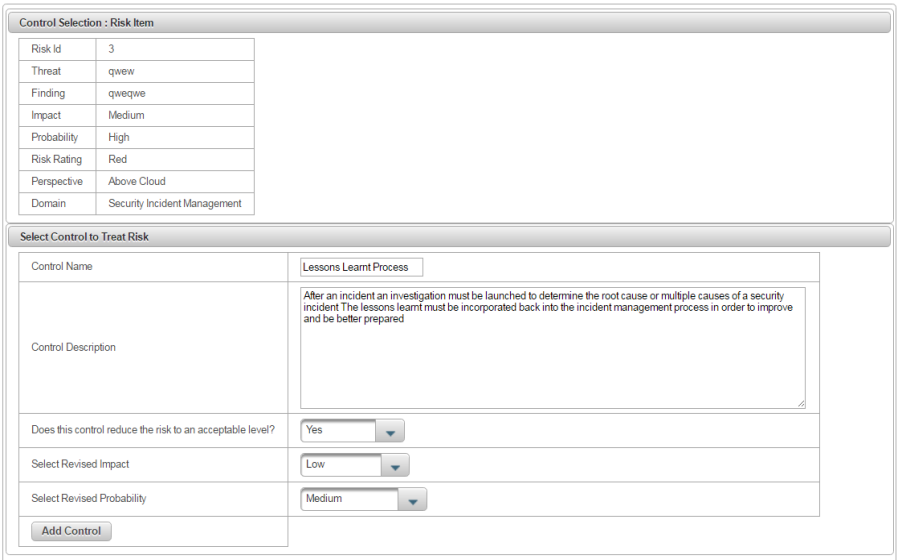

Figure 9 add the control and indicate new impact and probability values

3.4 Phase 4: Assessment Closeout

Phase 4 is a simple step. Once the assessment is complete and all threats have been provided controls, the facilitator can close out the assessment. The tool will set the assessment status to “Completed”.

Figure 10 Assessment Closeout

5. Metric Display in JSF

5.1 Overall Qualitative Risk Score

The Periculum Web Application visually shows the qualitative measurement in a meter gauge, and also counts the number of confidentiality, integrity and availability risk records in the risk register regardless of the status of the assessment associated with them.

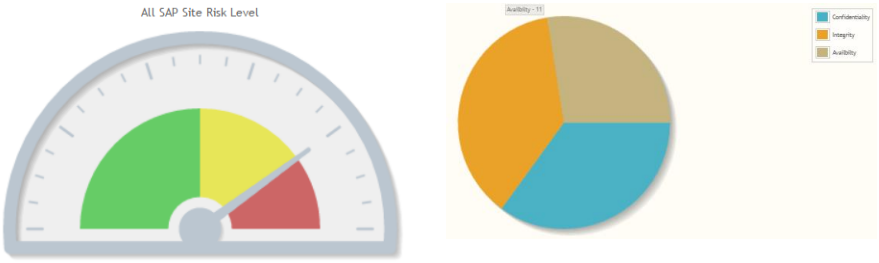

Figure 11 Overall Risk Status

5.2 Quantitative Risk Score per SAP Site

The second and last metric for the Risk Analysis Tool is to calculate the risk score per SAP Site and per domain. Figure 15 shows the breakdown and numbers calculate per domain with a final risk score at the bottom of the page.

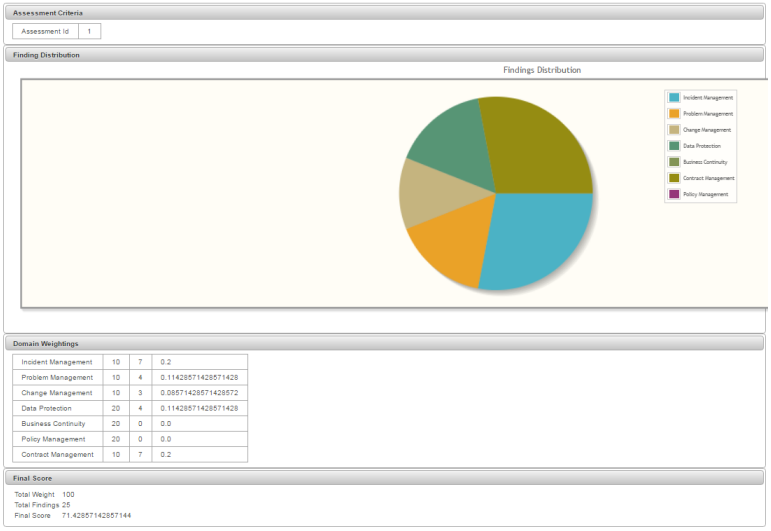

Figure 12 Quantitative Risk Score per SAP Site and Domain

6. Critical Evaluation of the implementation

The Risk analysis tool can be considered a beta version, which demonstrates the capability of a web based implementation of FRAAP to an extent. However, the implementation, in terms of the measurement of risks points of the three dimensional model is flawed in certain aspects.

In the following section, we discuss some of the main areas that requires a review and provide recommendations for improvement.

6.1 Overall Qualitative Risk Score

The overall qualitative risk score, merely adds the amount of red, yellow and green findings of all the assessments, and does not represent an accurate indication of risk.

The reason is that weightings has not been considered for Integrity, Availability and Confidentiality, nor the weightings for the seven dimensions implemented. One could have calculated the weighting for each domain, above and below the cloud, and then integrated weighting for Integrity, Availability and Confidentiality.

We can argue that the weighting for Availability from the perspective of the Cloud Provider is higher than Integrity and Confidentiality, since this would make business sense, and then on the other hand that Cloud Adopters might consider Confidentiality more important than Integrity and Availability, since their data would reside on the Cloud.

A recommendation is then made to instead, to formulate an equation which representative of the weights for the domains, as well as the business attributes of Confidentiality, Integrity and lastly Availability.

6.2 Quantitative Risk Score per SAP Site

The same argument holds for the quantitative calculation of the Risk Score per SAP Site. Even though weightings are considered for the seven domains, the weightings for Integrity, Availability and Confidentiality has been ignored.

A recommendation is that a formula is derived in order to weigh in the business attributes for Integrity, Availability and Confidentiality.

6.3 Compensating Control Selection

Although the Risk Register table includes a Compensating Control ID field, it is not used in the current version of the tool. Since risks cannot be 100% mitigated, it is important that compensating controls are used, which is similar and serves the same intent and rigor of the original control.

Adding the ability to incorporate compensating controls, provides the facilitator the means to lower risks even more, and provides a far more accurate view and measurement of the risks.

6.4 Risk Matrix

The risk matrix implemented might be too simplistic and does not necessarily represent the actual impact for Cloud Provider or Cloud Adopter. No research was performed on this aspect, since it was out of scope. However, potentially seeking a harmonised impact rating or alternatively providing the ability to add custom impact metrics, especially for Cloud Adopters (Above the Cloud) risks.

6.5 Risk Domains

The seven domains are hardcoded into the web application and database. This means that the facilitator is only limited to those. It would have been advantageous if the database and web application could have allowed the domains, which could be processes or technology, to be added dynamically, and be assessed within the same model.

A recommendation is made to allow dynamic creation of domains for risk assessment purposes, so that the risk analysis tool can be extended beyond the seven domains as listed.

6.5 Questionnaires

The risk analysis tool does not allow the facilitator to perform a gap assessment on the seven domains. This information could be very valuable during a FRAAP session and can provide background information on gaps in the area of assessment (domains), that would have otherwise have been unnoticed.

7. Areas for further research

In this section we provide some potential areas for further research taking into consideration of what the risk analysis tools' capability is currently:

7.1 Weighting Formulas

Considering the weighting aspects regarding the multi-dimensionality of the problem addressed, a formula must be developed or derived to calculate a score out of 100, regardless of the amount of perspectives or domains.

7.2 Harmonised Risk Matrix

The second area which require research is the formulation or development of either a harmonized risk matrix for both Cloud Adopter and Cloud Provider. This would provide a generic risk matrix to work with.

8. Conclusion

This research paper is an after-the-fact review of a Risk Analysis Tool called Periculum.

The risk analysis tool conceptually demonstrates the concept of a multi-dimensional attribute model for Cloud Provider and Cloud Adopter, as with SAP HEC, implemented in a web based tool. It is at no point a perfect tool. However, there are a few positive aspects, in that the data model, with a little modification and the JSF implementation with some modification, could potentially implement the model appropriately.

The tools' has been demonstrated and a critical evaluation provided in terms of the aspects that require a review or redesign and further research has been identified,

firstly weighting formulas that are appropriate to use, in the context of this model, and lastly a harmonised risk matrix, which potentially can provide a solid basis for risk calculations.

10. References

Baneth, A., 2015. Not all risks are created (and perceived) equal. Available online. http://www.baneth.eu/2015/09/22/not-all-risks-are-created-and-perceived-as-equal/. Accessed: 9 November 2015.

Clemen, R.T. and Winkler, R.L., 1999. Combining probability distributions from experts in risk analysis. Risk analysis, 19(2), pp.187-203.

Peltier, T.R., 2005. Information security risk analysis. CRC press.