# BUSINESS DRIVEN RISK ASSESSMENT
## *A Methodical Approach to Risk Assessment and Business Investment*

David W. Enström
*1246857 Ontario Ltd., 14 Honey Gables Dr., Ottawa, K1V 1H5, Canada*

Siavosh Hossendoust
*Enterprise Security Architect, IBM, 2220 Walkely Road, Ottawa, Canada*

Keywords: High Assurance Enterprise Security Architecture Risk Assessment Planning.

Abstract: Dynamic business environments require concurrent, distributed, and flexible architectures that must provide an agreeable level of reliability and acceptable level of trust. A three level undisruptive business driven planning process has been formulated using a risk analysis model that provides a justifiable direction for implementing a low risk solution and selecting appropriate products. The methodology includes identification of "Risk Priority" through assessment of risks for: business effectiveness, logical IT solution architecture (PIM) aspects, and physical IT solution architecture (PSM) aspects. It also introduces a risk dependency analysis process as an aid in understanding relationships between architectural layers. This proposed methodology aids in understanding and prioritizing risks within the context of the organization; it has broadened the concept of a TRA into a risk controlled solution architecture domain.

## 1 INTRODUCTION

This paper articulates a modern IT capability planning and acquisition process that fuses business and technology experts with best practices and lessons learned to increase synergy between capability acquisition and its support of business objectives. This is done through the assessment of risks in the context of business priorities, solution architecture options and technical solution options. A conceptual model for risk is developed along with characterization and analysis of business impact and architectural impact.

Traditionally, technology experts and project managers rely on their technology and domain knowledge, plus best practices, to compare solution options and plan investment. Undoubtedly, this kind of approach has produced many high–value lessons learned for solution architecture improvements, risk mitigation and planning that have not been exploited effectively. These lessons learned have evolved to the point where today there are widespread enterprise planning and architecture processes beneficial for large IT projects. These processes strive, through the application of proven methodologies and enforcing best practices, to provide quality product delivery that meets the business requirements. The use of these processes is proven to eliminate and mitigate investment and development risks, and also result in solutions that better meet the business need.

This paper describes a methodical approach for the assessment of risk based upon business priorities and goals, logical architecture aspects and physical architecture aspects with an aim to improve the cost–effectiveness and business benefits of corporate IT security investments.

## 2 RISK MODEL

The proposed process is dependent upon a thorough analysis of risk. Risk can be decomposed into three disjoint sets or categories, namely risk associated with business operations, risk associated with the chosen logical solution and risk associated with the physical solution implemented:

High priority risks are usually the ones of interest to the business and IT since they will have the



W. Enström D. and Hossendoust S. (2008).
BUSINESS DRIVEN RISK ASSESSMENT - A Methodical Approach to Risk Assessment and Business Investment.
In *Proceedings of the Tenth International Conference on Enterprise Information Systems - ISAS*, pages 271-278
DOI: 10.5220/0001701602710278

largest impact. It is therefore important to understand the relationship between risks at each of these architectural layers, at both initial capability design and implementation time and later in the system life–cycle.

Dependencies exist between business components (i.e. functions and processes), between logical architecture (Processing Independent Model (PIM)) components and between Physical level solution (Processing Specific Model (PSM)) components. Dependencies also exist between components at one layer (e.g. business) and other layers (e.g. PIM). For example, an important business process may rely on a server, and the server's life expectancy and availability are dependent on the reliability of its weakest component (e.g. hard drive or power supply). These dependencies need to be systematically analyzed in such a way that high priority (and some medium priority) risks can be identified and mitigated. Systematic prioritization (based upon business drivers) of these risks is done, which provides many benefits.

This Risk Dependency Analysis can be directly equated to Social Network Analysis, where in the risk context the nodes are *business*, *PIM* or *PSM* components and the relationships or ties between nodes are the risk dependencies as shown in Figure 1.

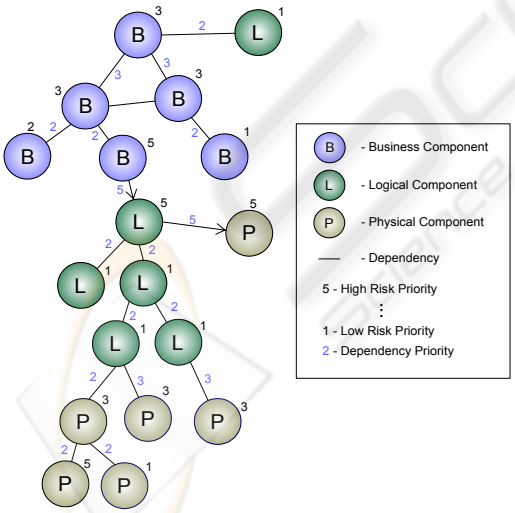


Figure 1: Risk Dependency Analysis Model.

## 3 RISK ASSESSMENT PROCESS

The process aims to define strategic IT plans in line with the business priorities through the definition of a more formal approach to the assessment of risks. This assessment process, summarized in Figure 2, is driven by business priorities along with an assessment of logical and physical component solutions. Therefore, each organization's specific situation and characteristics will be used to determine the most significant sources of business productivity, the business areas affected along with the risks that pose the highest impact and chance of happening.

The model in Figure 2 is used to define the relative risk priority based upon risks that have the highest business impact, which in turn drives the selection of technologies and solutions that are most useful for business. In other words, the impacts of risks plus constraints derived from the business is used to develop a comprehensive and low risk plan, which in turn leads to product selection choices that mitigate a given level of risks. This has the following benefits:

- Understanding the risk impact and risk priority allows selection of solutions appropriate and cost–effective for a given risk
- Risk impact analysis permit a more logical and appropriate phasing of implementation
- Design and technology choices, including costs, are easily justified based upon this type of risk analysis

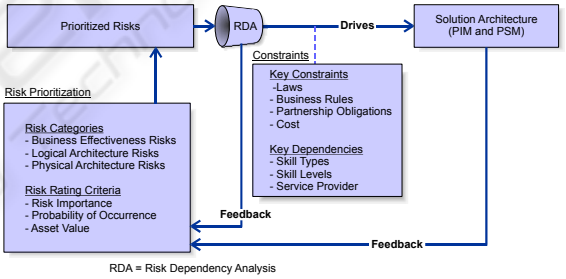


Figure 2: Business Driven Risk Analysis.

The Risk Prioritization portion of the model shown in Figure 2 is the key aspect of this business–driven approach. It will be described in more detail below. The Risk Dependency Analysis (RDA) is a refinement of available solution options (also see Figure 3), whereas constraints are conditions to which all solutions must comply.

## 4 RISK PRIORITIZATION

The prioritization of risks, based upon several methodical criteria, is the key to this process. The process for determining risk priority is applied to all identifiable risks. This process is used to assess all

types of risks. Risks are identified and evaluated based upon three categories:

- **Business Effectiveness Risks** – Risks that, if they were to occur, would harm the effectiveness of the business to accomplish it goals.
- **Logical Architecture (PIM) Risks** – Risks in this category are associated with the logical definition of the solution architecture, the lack of proper Identity Management for example.
- **Physical Architecture (PSM) Risks** – Risks in this category are associated with the physical definition of the solution architecture, the specific attributes of a technology in use for example.

These categories are defined further below.

## 4.1 Business Effectiveness Risks

Timely, accurate, and appropriately information gathering, flow, processing, analysis and secure distribution are needed to maintain business effectiveness. Consequently, for the organization to stay in business, it is necessary that it satisfy client, partner and vendor obligations. The following business capabilities are examined, among many others, to determine the level of risk involved for the various business areas

- Well defined and fully enforced business processes
- Undisrupted and high quality business services
- High quality services management:
- Timely access to valuable information
- Suitable communication channels at all levels
- Uninterrupted legitimate user access

## 4.2 Logical Architecture Risks

The logical architecture includes an end–to–end IT systems strategy for various aspects of the IT infrastructure and environment in accordance with the organizational (and partner) policies and business rules. Risks have significant importance in this context and must be rated appropriately by the IT and security subject matter experts.

The logical level architecture defines the approach for developers, which is evaluated to determine the level of risk involved for its various aspects. Some of the aspects of the logical architecture to be examined to identify risks are:

- User requirements
- Business use cases
- System use cases
- Architectural decisions
- Architectural models
- System requirements / specifications
- Policies and business rules
- Service / component aspects and structure
- Resource / content management
- Integration and interoperability

## 4.3 Physical Architecture Risks

The physical architecture must include an end–to–end IT product strategy for the IT environment, and in accordance with organizational (and perhaps partner) policies and business rules. Risks have significant importance in this context and must be rated appropriately by the IT and security subject matter experts.

The physical level (operational) risks such as “inadequate admin tools” and common risks such as “lack of timely product vendor information” are two major areas that must be dealt with. Aspects of the physical solution architecture to be examined, among many others, to identify risks are:

- System testing
- System deployment
- System configuration
- System connectivity
- System protection
- System life–cycle management
- Administration
- Product type, setup and configuration
- Product service and support
- Product maintenance
- Product assurance level

## 4.4 Risk Rating Criteria

In–order to understand and prioritize risk within these three contexts, it has been necessary to broaden the concepts of the formal Threat Risk Assessment (TRA). This has been achieved by introducing a risk rating technique known as the “Risk Priority”. Risk Priority is derived from three conditions, namely *Risk Importance*, *Risk Probability* and *Asset Value*. Each of these three conditions is described below, followed by an explanation of how they are used to calculate Risk Priority. The referenced tables are in the Appendix

Having a Risk Priority provides many benefits, including:

- The ability to make intelligent cost–benefit decisions
- The ability to choose protections appropriate for each risk within a specific business context
- The ability to prepare intelligent implementation planning and phasing decisions

### 4.4.1 Risk Importance

The risk importance rating defines the relative importance of the risk to the organization; based upon the threat and the organizational and business context. For example, a business that only sells online would place a very high risk importance on business, solution and physical components

supporting this portion of the business. Appendix Table 1 defines the ratings used for risk importance, along with specific criteria for determining the correct importance value. Ratings defined are from 1 (very low Risk Importance) to 5 (very high Risk Importance).

### 4.4.2 Risk Probability

The risk probability ratings, as described in Table 2, define the likelihood of a risk (threat) occurring. They are based upon the level of confidence of the organization in the capability of its users, the deployed environment, and organizational plans and processes; plus the vulnerability of the component that are characterized by the evaluator knowledge, assurance level and environmental protection. These two factors are what determine the likelihood of a risk (threat) actually occurring. Ratings defined are from 1 (very low Risk Probability) to 5 (very high Risk Probability).

### 4.4.3 Asset Value

The Asset Value rating is purely a business valued based assessment. The value of assets to the business (not necessarily their monetary value), involved or implicated in a specific risk/threat, define this rating. The Risk Importance is based upon the impact to the business of the risk occurring, the Asset Value amplifies this by defining the relative value of assets involved. For example, a business that only sells online would place a very high Asset Value on business, solution and physical components supporting this portion of the business. Table 2 defines the generic ratings for Asset Value. The ratings defined are from 1 (very low Asset Value) to 5 (very high Asset Value).

### 4.4.4 Risk Prioritization Calculation

Risk priority is a combination of the importance of the risk, and the probability of the risk occurring, and the value of the business assets involved.

The calculation of risk priority is quite simple:

***Risk Priority*** = *Risk Importance* x *Risk Probability* x *Asset Value*

The risk priority is calculated by multiplying together the three rating criterion. If the risk importance or risk probability are zero (the asset value should never be zero), then the priority is zero, meaning that no investment should take place to mitigate the associated risk. Similarly, if the risk importance is high and the risk probability is high, then a level of investment commensurate with the value of the business assets involved should be made. Thus, once the Risk Priority is determined, it is used to decide on the level of effort and expense that should be applied in mitigating the risk, and in the priority for implementation of safeguards.

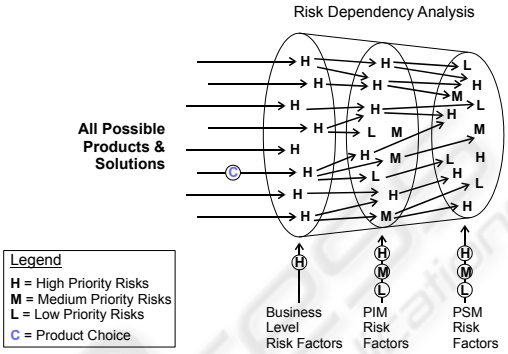


Figure 3: Solution Analysis: RDA vs. Solutions.

## 4.5 Solution Analysis

Figure 3 illustrates how analysis is used to finalize capability planning and to select best products. The potential candidate products from each optional solution for physical architecture are examined to determine what risks they mitigate at the business level. This reduces further the possible set of candidate products. Likewise, candidate solutions are then examined to determine what risks they also address at the PIM level. As shown in the diagram, a solution to a business level risk will ideally address multiple risks at the PIM level, and even more at the PSM level. The solution is chosen that addresses the most risks at all levels, all other factors (e.g. cost and life–cycle cost) being equal. Some, hopefully low level, risks may not be addressed by any solutions, in which case the risk must be accepted by business management, or changes will need to be made to the architecture to reduce or eliminate these risks.

# 5 EXAMPLE

## 5.1 Simple Scenario

A modern datacenter for a global business is located in a city that is known for ice storms. Ice storms seriously affect the A/C power supply, among other infrastructure services. The loss of power is a serious business risk that impacts business obligations (e.g. services uptime for customers must be equal or

better than 99.5 %). This situation is analysed below following the described approach.

The Risk Importance rating is three (3) since it will have an "important impact (denial of service beyond agreeable delays, partners affected)" from Table 1.

The Risk Probably rating is four (4) since there is "Inadequate ability within the organization, or with current technology, to reduce or manage the risk impact" from Table 2.

The Asset Value rating is five (5) since the "affected asset(s) is extremely important to day–to–day business activity" from the Table 3.

Following the formula described above, the Risk Priority for this particular risk is:

$$\textbf{\textit{Risk Priority}} = 3 \times 4 \times 5 = 60$$

The real advantage to the business comes when multiple risks are prioritised and Risk Dependency Analysis is done, allowing informed investment decisions to be made.

# 6 SUMMARY AND CONCLUSIONS

## 6.1 Summary

The purpose of the process is to acquire IT security solutions that mitigate risks at the appropriate level and in line with business priorities. The logical architecture and technical solution are also included in the analysis. Life cycle costs and skills demand should also be factored in to provide a complete view of the solution. The significant stakeholders for this approach are following groups:

1. Business mission management groups
2. IT planning & strategy groups
3. IT support & operations groups

Advantages of the proposed approach are:

1. Business evolution aided by methodical threat risk assessment processes
2. Systematic prioritization resulting in cost effective and appropriate investment
3. Repeatable analyses that are important for evaluating architecture and solution options
4. Ability to validate the solution is in support of the right business needs / priorities
5. Validation of the technical priorities in relation to business priorities
6. Ability to compare alternative solution options from multiple project aspects

Disadvantages of the proposed approach are:

1. Lack of standards for business prioritization process
2. Dependent upon domain expert knowledge
3. Dependent upon the accuracy of the business priorities
4. Dependent upon the quality of the logical and physical architectures

## 6.2 Related Work

There is little work closely related to this analysis approach. The (McGraw, 2006a and 2006b) article and book summarize well the current activity, and references some similar concepts; however this paper broadens the definition of risk analysis so that it includes multiple architectural layers, including the business layer. It also shows how these architectural layers may be related and understood through Risk Dependency Analysis.

Similarly, (Kotonya) explores the usage of risk analysis during development, but leaves out the critical link to business requirements and business plans.

Another similar approach by Robert Benedict (NASA, 2003) shows risk analysis as part of a sound business plan and its benefit to the Agency in developing (and will be fully coordinated with the ongoing effort to define) the NASA Enterprise Architecture. Again, Michael G. Stamatelatos (NASA, 2004) leaves out logical level and physical level risks.

## 6.3 Future Work

Historically, the most common projects are those that do not transform the business completely, do not conflict with the enterprise architecture and do not require noticeable changes to the infrastructure. Recently, the evolution of new architectural frameworks such as Service Oriented Architecture (SOA) and Model Driven Architecture (MDA) are providing the ability to make rapid changes at business, architecture and infrastructure levels.

As always, practitioners who are specialist in their domain and very likely familiar with theses frameworks still need a systematic and repeatable process that helps them to make timely, effective and low risk capability planning decisions. Generally, the current common concerns are "How do we get there?" and "How do we do that?" We have explained within this document, through a systematic and repeatable process, "How we get

there". We will discuss a systematic process "how we do that" in future work.

### 6.4 Conclusions

The systematic and repeatable process allows capability planners to develop and prioritize capabilities and assess the gain/ impact before making project proposals or even making serious investments.

The feedback from program managers that have used this process for large project capability planning (projects that continue for several years) have been very positive and they have confirmed that application and demonstration of this process as part of their capability planning has increased the creditability of their plans.

## ACKNOWLEDGEMENTS

Authors would like to express sincere gratitude to Dr. D. Walsh for his innovative leadership.

## REFERENCES

CSE, (2005). *Threat and Risk Assessment Working Guide,* viewed January 2007, <http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg04-e.html>.

McGraw, Gary (2006a). *Software Security: Building Security In,* Addison–Wesley, New York.

McGraw, Gary (2006b). *Architectural Risk Analysis,* Viewed November 2007, <http://www.devsource.com/article2/0,1895,1928687,00.asp>.

IBM (2003). *Risk reduction with the RUP phase plan*, Viewed November 2007, <http://www.ibm.com/developerworks/rational/library/1826.html>.

HP (2007). *Planning for Disaster: Assessing Risks to Your Business Data*, Viewed November 2007, <http://www.score.org/pdf/HP_Download_PlanningforDisaster.pdf>.

Kotonya, Gerald, & Rashid, Awais (2001). A Strategy for Managing Risk in Component–based Software Development. *Proceedings of the 27th EUROMICRO Conference 2001: A Net Odyssey (EUROMICRO'01)*, pp. 12-22.

NASA (2003). *XML Business Case*, Robert Benedict, NASA, Washington.

NASA (2004). NASA Activities in Risk Assessment, *Project Management Conference 2004*, Michael G. Stamatelatos, NASA, Washington.

Houmb, S.H., Georg, G., France, R., Bieman, J., Jurjens, J. (2005). Cost-benefit trade-off analysis using BBN for aspect-oriented risk-driven development. *Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems,* pp. 195-204.

Williams, Ray, Ambrose, Kate, Bentrem, Laura, Merendino, Tom (2004). *Risk Based Diagnostics*, Carnegie Mellon Software Engineering Institute for the Department of Defense, Pittsburgh.

Choudhary, A. Rahim, (2005). A Policy Based Architecture for NSA RAdAC Model. *Proceedings of the 6th IEEE IA Workshop*, pp. 10.

Wikipedia (2007). *Social Network*, Viewed November 2007, http://en.wikipedia.org/wiki/Social_network_analysis.

The Bumble Bee (2006). *Social Network Analysis: An Introduction,* Viewed November 2007, <http://www.bioteams.com/2006/03/28/social_network_analysis.html>.

Liemur (2005). *Risk Based Software Development: Reducing Risk and Increasing the Probability of Project Success*, Viewed November 2007, <http://www.liemur.com/Articles/Risk_Based_Software_Development.html>.

Custers, B. H. M. (2007). Risk Profiling of Money Laundering and Terrorism Funding - Practical Problems of Current Information Strategies. *ICEIS 2007 Conference Proceedings*, pp. 90-94.

Gulías, Víctor M., Abalde, Carlos, Castro, Laura M., Varela, Carlos (2006). Formalisation of a Functional Risk Management System. *ICEIS 2006 Conference Proceedings*, pp. 516-519.

Misra, Subhas C., Kumar, Vinod, Kumar, Uma (2005). Modeling Strategic Actor Relationships to Support Risk Analysis and Control in Software Projects. *ICEIS 2005 Conference Proceedings*, pp. 288-293.

Enström, David W., Walsh, D'Arcy, Hossendoust, Siavosh (2007). A Reference Model for Enterprise Security - High Assurance Enterprise Security. *ICEIS 2007 Conference Proceedings*, pp. 355-364

# APPENDIX

Table 1: Risk Importance Ratings.

| Business Effectiveness | Effected Users | Rating |
|---|---|---|
| Minor impact (e.g. short interruption) | Minor impact (less than 1% of users)<br>*and*<br>Minor exposure: Effects of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited. | **1** |
| Moderate impact (e.g. management agreeable delays / interruption in services) | Moderate impact (deemed essential employees and management can continue their work)<br>*and*<br>Moderate exposure: Vulnerability can be expected to affect more then one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited. | **2** |
| Important impact (denial of service beyond agreeable delays, partners affected) | Important impact (essential employees and management are effected, plus partners)<br>*and*<br>Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited. | **3** |
| High impact (denial of service beyond agreeable delays, clients affected) | High impact (essential employees and management are effected, plus clients)<br>*and*<br>Vulnerability affects a majority of client facing system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited. | **4** |
| Extreme impact (the future of the business is at stake) | Extreme impact (all employees, clients and partners affected)<br>*and*<br>Vulnerability affects the viability of continued operations.<br>Exploitation significantly increases the probability of additional vulnerabilities being exploited. | **5** |

Table 2: Risk Probability Ratings.

| Confidence in Users, Systems & Organizational Processes | Vulnerability Level | Rating |
|---|---|---|
| **Confidence: High**<br>***High Confidence Indicators***<br>User: Has extensive knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, without causing damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build to specification and composed of matured components.<br>*And*<br>**Organization**: Both tested recovery and business continuity plans exist in the organization to manage the risk impact and maintain business continuity. | **Vulnerability: Low**<br>***Low Vulnerability Indicators***<br>**Evaluator**: Has extensive domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**Capability**: Evaluated to an appropriate level of assurance, certified and deployed following industry recommendations.<br>*And*<br>**Environment**: has suitable level of protection. | **1** |
| **Confidence: High**<br>***High Confidence Indicators***<br>**User**: Has extensive knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, without causing damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build to specification and composed of matured components.<br>*And*<br>**Organization**: Both tested recovery and business continuity plans exist in the organization to manage the risk impact and maintain business continuity. | **Vulnerability: Medium**<br>***Medium Vulnerability Indicators***<br>**Evaluator**: Has domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**Capability**: Evaluated to an appropriate level of assurance, vulnerabilities mitigated and deployed following industry recommendations.<br>*And*<br>**Environment**: has acceptable level of protection. | **2** |
| **Confidence: High**<br>***High Confidence Indicators***<br>**User**: Has extensive knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, without causing damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build to specification and composed of matured components.<br>*And*<br>**Organization**: Both tested recovery and business continuity plans exist in the organization to manage the risk impact and maintain business continuity. | **Vulnerability: High**<br>***Medium Vulnerability Indicators***<br>**Evaluator**: Has limited domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**Capability**: Limited testing only, identified vulnerabilities mitigated and deployed following industry recommendations.<br>*And*<br>**Environment**: has low level of protection. | **3** |
| **Confidence: Medium**<br>***Medium Confidence Indicators***<br>**User**: Has adequate knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, without causing damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build to specification and composed of tested components.<br>*And*<br>**Organization**: Recovery and business continuity plans to manage the risk impact and maintain business continuity exist in the organization but not tested. | **Vulnerability: Low**<br>***Low Vulnerability Indicators***<br>**Evaluator**: Has extensive domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**System**: Evaluated to an appropriate level of assurance, certified and deployed following industry recommendations.<br>*And*<br>**Environment**: has suitable level of protection. | **2** |

Table 2: Risk Probability Ratings (cont.).

| Confidence in Users, Systems & Organizational Processes | Vulnerability Level | Rating |
|---|---|---|
| **Confidence: Medium**<br>***Medium Confidence Indicators***<br>**User**: Has adequate knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, without causing damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build to specification and composed of tested components.<br>*And*<br>**Organization**: Recovery and business continuity plans to manage the risk impact and maintain business continuity exist in the organization but not tested. | **Vulnerability: Medium**<br>***Medium Vulnerability Indicators***<br>**Evaluator**: Has domain knowledge and expertise to perform relatively accurate evaluation and provide mitigation plan.<br>*And*<br>**System**: Evaluated to an appropriate level of assurance, vulnerabilities mitigated and deployed following industry recommendations.<br>*And*<br>**Environment**: has acceptable level of protection. | **3** |
| **Confidence: Medium**<br>***Medium Confidence Indicators***<br>**User**: Has adequate knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, without causing damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build to specification and composed of tested components.<br>**Organization**: Both recovery and business continuity plans to manage the risk impact and maintain business continuity exist in the organization but not tested. | **Vulnerability: High**<br>***Medium Vulnerability Indicators***<br>**Evaluator**: Has limited domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**System**: Limited testing only, identified vulnerabilities mitigated and deployed following industry recommendations.<br>*And*<br>**Environment**: has low level of protection. | **4** |
| **Confidence: Low**<br>***Low Confidence Indicators***<br>**User**: Has limited knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, and may cause damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build as you go with limited testing.<br>*And*<br>**Organization**: Both recovery and business continuity plans to manage the risk impact and maintain business continuity do not exist in the organization. | **Vulnerability: Low**<br>***Low Vulnerability Indicators***<br>**Evaluator**: Has extensive domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**System**: Evaluated to an appropriate level of assurance, certified and deployed following industry recommendations.<br>*And*<br>**Environment**: has suitable level of protection. | **3** |
| **Confidence: Low**<br>***Low Confidence Indicators***<br>**User**: Has limited knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, and may cause damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build as you go with limited testing.<br>*And*<br>**Organization**: Both recovery and business continuity plans to manage the risk impact and maintain business continuity do not exist in the organization. | **Vulnerability: Medium**<br>***Medium Vulnerability Indicators***<br>**Evaluator**: Has domain knowledge and expertise to perform relatively accurate evaluation and provide mitigation plan.<br>*And*<br>**System**: Evaluated to an appropriate level of assurance, vulnerabilities mitigated and deployed following industry recommendations.<br>*And*<br>**Environment**: has acceptable level of protection. | **4** |
| **Confidence: Low**<br>***Low Confidence Indicators***<br>**User**: Has limited knowledge, skills and knowledge of the organization's processes, roles and responsibilities and infrastructure to use authorized services, and may cause damage to reputation or effectiveness of the business.<br>*And*<br>**Capability**: Build as you go with limited testing.<br>*And*<br>**Organization**: Both recovery and business continuity plans to manage the risk impact and maintain business continuity do not exist in the organization. | **Vulnerability: High**<br>***Medium Vulnerability Indicators***<br>**Evaluator**: Has limited domain knowledge and expertise to perform accurate evaluation and provide mitigation plan.<br>*And*<br>**System**: Limited testing only, identified vulnerabilities mitigated and deployed following industry recommendations.<br>*And*<br>**Environment**: has low level of protection. | **5** |

Table 3: Asset Value Ratings.

| Business Impact | Asset Context | Rating |
|---|---|---|
| Affected asset not important to day–to–day activity | No dependency between the affected asset(s) and other assets | **1** |
| Affected asset moderately important to business activity. | Moderate dependency between the affected and other asset(s) | **2** |
| Affected asset important to day–to–day activity | Important dependency between the affected and other asset(s) | **3** |
| Affected asset highly important to day–to–day activity | High dependency between the affected asset(s) and other assets | **4** |
| Affected asset extremely important to business activity | Extreme dependency between the affected and other asset(s) | **5** |