A Risk Assessment Report for Acme Manufacturing

Risk Assessment Methods

Many risk assessment frameworks, practices and methods are available to address cybersecurity and technology-related risks. However, Woody (2006) argues several factors such as the organization's future-looking plans, objectives, goals, management practices, and legislative requirements that need to be considered before deciding on potential risk assessment methods and even further tailoring them to the needs of the organization. Therefore, these factors, including the list of assumptions mentioned in the previous paper, will be considered while comparing the differences of available risk assessment methods. (Duricu, 2019; Wangen, 2018) states the Core Unified Risk Framework (CURF) offers a reliable approach when comparing different risk assessment methodologies. CURF includes a detailed and comprehensive comparison of nine risk assessment methods. Thus, our analysis below follows this well-structured approach and compares the most promising three risk assessment methodologies called OCTAVE, ISO/IEC 27005:2011 and NIST 800-30.

Scoring interpreted in a following way: XX =2, X=1, - =0

Score	Description	
XX	Addressed	A task is fully addressed with clear descriptions of how to solve it.
X	Partially addressed	A task is suggested but not substantiated
-	Not addressed	The methods do not mention or address a particular task at all.

Table 1 - CURF Score Description

Set of Criteria	Octave	ISO 27005	NIST 800-30
Risk Identification			
Preliminary assessment	XX	-	XX
Risk criteria determination	XX	XX	-
Business objectives	XX	XX	-
Cloud-specific consideration	-	-	X
Key risk indicators	-	-	-
Stakeholder identification	X	XX	-
Stakeholder analysis	-	-	-
Asset identification	XX	XX	-
Mapping sensitive data	X	X	X
Asset evaluation	X	X	X
Asset owner	XX	XX	-
Asset container	XX	-	-
Business processes	-	XX	X
Vulnerability management	X	XX	XX
Vulnerability assessment	-	XX	XX
Threat identification	XX	XX	XX
Threat assessment	XX	XX	XX
Control identification	X	XX	XX
Control assessment	-	XX	-
Outcome identification	XX	XX	XX
Outcome assessment	X	XX	-
Risk Estimation			
Asset identification and evaluation	-	-	X
Threat willingness/motivation	XX	XX	XX
Threat capability (know how)	-	X	XX
Threat capacity (Resources)	X	X	-
Threat attack duration	-	-	-
Vulnerability assessment	-	-	XX
Qualitative Probability Estimation	X	XX	XX
Quantitative Probability Estimation	-	XX	XX
Qualitative Impact Estimation	X	XX	-
Quantitative Impact Estimation	XX	XX	XX
Level of risk determination	-	XX	-
Risk aggregation	X	XX	XX
Risk Evaluation			
Risk criteria assessment/revision	X	X	-
Risk prioritization/evaluation	XX	XX	XX
Risk treatment recommendation	XX	-	-
Completeness			
Process	**Octave**	**ISO 27005**	**NIST 800-30**
Risk Identification	24	30	18
Risk Estimation	8	16	15
Risk Evaluation	5	3	2
Completeness total score	37	49	35

Table 2 - CURF, Main qualitative differences between frameworks

Table 2 contains all of the standalone tasks which are part of the risk assessment methodologies and are based on Wangen et al. (2018) work. At first glance, ISO/IEC 27005 marked as the highest scorer due to addressing most standalone tasks listed in Table 2. Duricu (2019) argues ISO/IEC 27005 has the highest level of completeness and includes well-known industry best practices, and risk

identification is one of the areas the framework excels. Additionally, Duricu (2019) also states OCTAVE does not meet some of the standalone tasks and requirements listed in Table 2, such as vulnerability and control assessments - thus, lead to immature risk estimation outputs. Moreover, heavily depending on excel-based worksheets to proceed further makes it hard to adopt by organisations. Therefore, our risk consultants recommend following ISO/IEC 27005 framework and risk assessment method for Acme Manufacturing.

Risk Analyses

	A COTS (Commercial Off the Shelf) solution	An Open-Source solution	An in-house created solution
Qualitative analysis	On the price of the managed service provider we will be in fact having certified expertise for the specific product. One of the risks in such a situation is to exceed the budget for new product deployment for the company.	The qualitative risk of the open source solution is that it is predominantly backed by an open source community as well as in house IT department. For any specific niche issue, it is likely that it might take more time to solve. High severity outages are highly unlikely to be present due to the big community of open source software.	The qualitative risk in such a situation is that the student implementing the in-house solution does not have the real live experience for developing a viable ERP for the business. As a main resource planning software for the business it is highly likely that the impact an issue can have can be major on the business.
Quantitative analysis	On the same aspect the Managed Service Provider needs to cover for the additional manpower needed to support such service meaning the risk of not having qualified personal is transferred to the MSP and removed from Acme Manufacturing	As for the in-house IT department need to be trained and will in fact need additional resources to be brought up to speed with the open source software as well as day to day operation of the platform.	Int terms of support personal this still needs to be supported by the IT team of the Acme Manufacturing now without a community to back the testing up as well as with a single point of failure where the knowledge is on the student that will develop the software
Risk treatment	The risk ownership of personnel is transferred to the MSP but the risk of exceeding the budget is still owned by the Acme Manufacturing.	In such situation the risk is moderate and supported by the Acme Manufacturing which in this case ownership cannot be transferred but removed by the vast community of open source software supporters and backed up by contribution from government institutions such as the EU (Open source software strategy, 2021)	In such a situation the risk is fully supported by the Acme Manufacturing company without the support of the community of an open source software relying only on the student developing the application as well as the IT department.

LIKELIHOOD	CONSEQUENCES				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Risk Matrix according to C. Simmons (2021)

Common Vulnerability Scoring System (CVSS)

The common vulnerability scoring (CVSS) system is a numerical risk level estimation model, which is maintained by the Forum of Incident response and security teams (FIRST) was introduced in 2004 and is currently on its third version, released in June 2019 (Houmb, Franqueira and Engum, 2009)

Consequently, the CVSS delivers a quantitative illustration of the information security vulnerabilities posed to Acme Manufacturing, as a result of the adoption of the ERP system operated by an open-source solution configured by the in-house IT division with reliance on the community forum for escalation support. This enables the IT department of Acme Manufacturing to differentiate between the vulnerabilities associated with the ERP open-source system, in order to prioritize the remediation of the threats which cultivates a favorable disaster recovery and business continuity plan for the company, whilst allocating financial resources efficiently.

The base metric group in the table below, adapted from (CVSS v3.1 Specification Document, 2021) signifies the fundamental features of the vulnerability and do not change over time. The base metric is calculated from the exploitability and impact metrics.

Basic Metric Group		**Temporal Metric Group**	**Environmental Metric Group**
Exploitability Metrics	Impact Metrics	Exploit Code maturity	Confidentiality Requirement
Attack Vector	Compatibility Impact	Remediation Level	Integrity Requirement
Privileges Required	Integrity Impact	Report Confidence	Availability Requirement
User Interaction	Availability Impact	-	Modified Base metrics
Scope	Scope	-	Security Requirements

The impact metrics measure the impact of the fruitfully compromised vulnerability.

CVSS Impact Metrics	Definition
Confidentiality	This metric increases as a result of the malicious attacker gaining unauthorized access to the ERP System and its private files.
Integrity	This metric increases when the attacker manipulates sensitive information on the ERP system.
Availability	This metric increases when the ERP system is unable to render it's intended service to Acme Manufacturing and is not accessible for authorized users.

The temporal metrics capture state of manipulation techniques in the vulnerability.

CVSS Temporal Metrics	Definition
Exploit Code Maturity	This metric increases as the malicious code to exploit the ERP open-source software system becomes more widely available to cybercriminals.
Remediation Level	This metric increases as patches or software updates to rectify a vulnerability in the ERP system become less available.
Report and Confidence	This metric is a measure of the specialist or technical knowledge in carrying out the vulnerability, which is available to cybercriminals.

Exploitability metrics defined below are scored comparative to the vulnerability.

CVSS Exploitability Metrics	Definition
Attack Vector	This metric reveals the situation whereby vulnerability manipulation occurs. The attack vector will increase as a threat becomes more remotely exploitable.
Attack Complexity	This metric outlines the prerequisites for vulnerability exploitation outside of the attacker's control. The attack complexity increases for exploits which require more information about the victim.
Privileges required	This metric defines the required tier of privileges an attacker must have to carry out an attack. The score for privileges required will increase with the level of administrative privileges needed to conduct an attack.
User Interaction	This metric requires the prerequisite of a malicious actor aside from the attacker to participate in the attack. The score is higher if the attacker can operate independently.

Qualitative Severity Rating Scale

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Qualitative Threat Guidance

Threat	CVSS Score	Severity Level	Guidance
Denial of Service Attack on the ERP network	9.5	Critical	Risk reduction with an intrusion detection system as a mitigation.
Unauthorized access of confidential files on the ERP system	9.2	Critical	Risk reduction with the use of strong and frequently reviewed passwords as a mitigation.
Compromise of sensitive supplier information due to undefined access control mechanisms.	9.0	Critical	Risk reduction with explicitly defined access controls as a mitigation.
Social engineering attacks due to inadequate employee training on the use of ERP systems.	8.6	High	Risk Reduction with adequate employee training on use of the ERP system as a mitigation
The injection of malicious code in the ERP open-source system.	8.2	High	Risk Reduction with qualified in-house computer programmers as a mitigation.

Denial of Service attack on the ERP system network

(Campbell, 2016) explains that a denial-of-service attack arises when a service, such as the ERP system becomes inoperable due to a malicious incident. (Brody and Kearns, 2009) state that ERP systems are particularly susceptible to cyber-attacks. In the event of a denial-of-service attack, the ERP system which holds all the confidential supply chain information of Acme Manufacturing will be non-operational for several hours or days (Crumbley *et al*., 2007). This reflects a large attack vector and security requirement as the availability of the ERP system is inhibited for working use, thereby reflecting a critical severity level.

Unauthorized access of confidential files on the ERP system

(Brody and Kearns, 2009) maintain that ERP systems transform the organizational hierarchy and manner in which corporations such as Acme Manufacturing operate, with the majority of tasks delegated to junior level workers. Consequently, employee privileges and access to private information must be assessed to ensure that passwords are adequately resilient and reviewed on a monthly basis. This safeguards against the critical severity of a disgruntled employee accessing confidential documents on the company's spork production plans, thereby minimizing the attack vector of the vulnerability whilst upholding the confidentiality, integrity, and availability of the ERP system (CVSS v3.1 Specification Document, 2021).

Compromise of Sensitive Supplier information due to undefined access control mechanisms

Enterprises such as Acme Manufacturing which implement the ERP system experience a broad matrix of users as the spork inventory and production departments are combined to achieve efficient management of its supply chain (Brody and Kearns, 2009). This gives rise to the occurrence of a spork production worker accessing confidential supplier information in the production module of the ERP system. Employee access privileges must be reviewed to guarantee adequate segregation of duties to curb the incidence of malpractice and a critical threat severity level.

Social engineering attacks due to inadequate employee training on the use of ERP systems.

(Hadnagy, 2018) postulates that social engineering is the practice of influencing an individual to perform an action which may not be in the person's best interests in order to divulge information. (Brody and Kearns, 2009) explain that ERP systems necessitate significant employee training to comprehend the obligations and duties which presents a significant financial investment for Acme Manufacturing. Subsequently, employees associated with the ERP system are often inadequately trained, which gives rise to social engineering pretexting attacks.

(Hadnagy, 2018) states that pretexting is the creation of a fabricated scenario by a malicious actor, to convince a targeted employee working on the inventory module of the Acme Manufacturing ERP system to divulge personally identifiable information about suppliers. This threat depicts a high severity level, as miniscule privileges are required to carry out the attack.

The injection of malicious code in the ERP open-source system.

It must be noted that open-source software code is accessible to anyone who wishes to access it. (Rodriguez and Gürcay, 2020) explain that the code of the open-source ERP system is accessible to malicious attackers who can foster specialist techniques to inject malicious code in the ERP system to compromise private data. This threat reflects a high severity level as the exploit code maturity facet of the threat increases.

Risk Reduction

(Sutton, 2014) states that risk reduction employs preventative and corrective controls which can be physical or technical, such as security locks and firewalls. Furthermore, risk reduction employs directive controls which are procedural consisting of security standards, and detective controls which can be physical, and technical controls such as intrusion detection systems.

Vendor Lock-in

(Rodriguez and Gürcay, 2020) explain that in terms of vendor lock-in, Acme Manufacturing will not be obliged to have a fixed software provider as a result of adopting the open-source ERP system. Support escalation will be available for the ERP open-source system as long as the community is in operation.

However, if the community that provides the support escalations desists from the project, this results in negative consequences which may affect the integrity and availability of the ERP system.

Cost-benefit Analyses

(Badewi & Shehab, 2013) argues there are different ways to evaluate ERP implementations, and these could be categorized into a couple of groups. These are briefly financial and qualitative models. Although perceiving different results, both models could possibly have valid use cases. However, qualitative models are not preferred over financial models due to not covering the implementation cost of projects in a detailed manner, including lack of understanding on management level. Therefore, the cost-benefit analysis section of the report will focus on financial models and take into consideration previously identified potential risks.

(Morgan, 2005; Wu et al., 2008) states NPV (Net Present Value) approach could be further used to combine financial risks, benefits and costs. (Badewi & Shehab, 2013)'s work and illustration below (figure 1) describes ERP performance lifecycles, including the NVP approach.

Badewi and Shehab

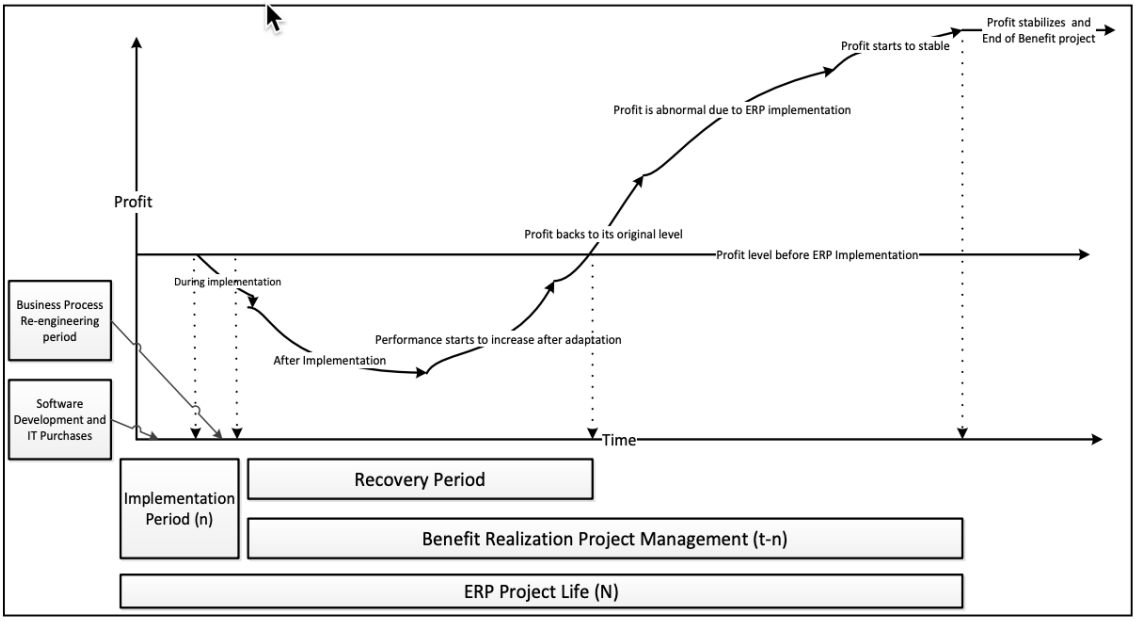

Figure 1: ERP Performance Lifecycle

Previously identified potential risks could be categorized under the following sections.

BPRI: Business Process Re-engineering Investment: Includes the training and advisory support costs, existing business processes, readiness and capabilities of the IT, and how fast the employees adapt to the changing environment.
SWI: Software Investment: Includes software acquisition, customisation, advisory support, configuration, hardening, activation and de-activation of systems.
HWI: Hardware Investment: Includes infrastructure-level costs

Additionally, Table 4 below illustrates potential costs and challenges for each of the available solutions, including potential cost levels.

Solution / Cost & Challenges	A COTS (Commercial Off the Shelf) solution	An Open-Source solution	An in-house created solution
High one-off investment	XX	-	-
Cash-flow challenges	X	-	-
Exceeding the budgeting	XX	-	-
Telephone support	X	XX	XX
Skills, Knowledge, Experience	-	X	XX
Resistance to change	X	X	X
High employee turnover	-	X	X
Incapable IT Dept.	-	X	X
Specific HW Requirements	X	-	-
Partially supporting business needs	-	X	X
Lack of support during Disaster	-	X	X
Security Vulnerabilities	-	X	XX
Operational Inefficiencies	-	X	X
Recruiting Project Manager	-	-	XX
Quality Assurance requirements	-	-	XX
Unexperienced internal IT Dept.	-	X	X
Implementation challenges	-	X	XX
Regular code reviews	-	X	XX
High maintenance cost	-	-	XX
Potential Cost Level	**High**	**Moderate**	**Low**

Table 4 – Potential cost level of available options – ACME Manufacturing

Recommended Option and Disaster Recovery Solution

As a recommended option based on the research done so far we would suggest Acme Manufacturing proceed with the Open-Source solution that will be installed and supported by their internal IT department, relying on community (forum) support for any escalations.

Open-source solution

For the purpose of adopting an ERP system, Acme manufacturing might maintain an open-source solution (OSS) at a low cost. Pankaja et al 2013 State that firms are capable of utilizing OSS with no need of paying for subscriptions, activation or any kind of set up.

According to AlMarzouq et al. 2005, reliability would play a vital role to maintain open-source software, at the time OSS can indicate high-level reliability, an unlimited number of developers support its community. As a result, acme manufacturing is capable of benefiting the cost of maintenance and upgrading.

Disaster Recovery

(Sutton, 2014) explains that disaster recovery is a specialized subsection of business continuity and outlines the provisions required to achieve the recovery of the ERP system.

As independent risk consultants to Acme Manufacturing, we recommend the use of warm standby platforms which have crucial applications configured with back up data.

Warm standby platforms are more costly than cold standby systems with the advantage of being brought back to regular operational use more swiftly.

Business Continuity

Business continuity is the ability of Acme Manufacturing to persist in its production of sporks at a satisfactory level following a damaging occurrence (Sutton, 2014).
Terms associated with business continuity such as the recovery point objective (RPO) which is the level whereby information used by the ERP system must be restored to allow for operation upon recommencement.
The recovery time objective (RTO) is the amount of time after an incident whereby the required services or resources of the ERP system must be recovered.

References

Duricu, A., 2019. [online] Diva-portal.org. Available at: https://www.diva-portal.org/smash/get/diva2:1323137/FULLTEXT02 [Accessed 16 December 2021].

Wangen, G., Hallstensen, C. and Snekkenes, E., 2018. A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6), pp.681-699.

Badewi, A. and Shehab, E., 2013, September. Cost, Benefit, and Financiall Risk (CoBeFR) of ERP Implementation. In Proceedings of the 11th International Conference on Manufacturing Research (ICMR2013), Cranfield University (pp. 19-20).

Morgan, J.N., 2005. A roadmap of financial measures for IT project ROI. IT professional, 7(1), pp.52-57.

Wu, L.C., Ong, C.S. and Hsu, Y.W., 2008. Active ERP implementation management: A Real Options perspective. Journal of Systems and Software, 81(6), pp.1039-1050.

C. Simmons, D., 2021. Qualitative and quantitative approaches to risk assessment. [online] Drmkc.jrc.ec.europa.eu. Available at: https://drmkc.jrc.ec.europa.eu/portals/0/Knowledge/ScienceforDRM/ch02/ch02_subch0201.pdf [Accessed 16 December 2021].

European Commission - European Commission. 2021. Open source software strategy. [online] Available at: https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en [Accessed 16 December 2021].

Fikri, M., Putra, F., Suryanto, Y. and Ramli, K., (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. Procedia Computer Science, 161, pp.1206-1215.

Syalim, A., Hori, Y. and Sakurai, K., 2009. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. 2009 International Conference on Availability, Reliability and Security,.

National Information Security Agency, 2012. Guide for Conducting Risk Assessments. Gaithersburg: Computer Security Division Information Technology Laboratory National Institute of Standards and Technology.

AlMarzouq, M., Zheng, L., Rong, G. and Grover, V., 2005. Open Source: Concepts, Benefits, and Challenges. Communications of the Association for Information Systems, 16.

Pankaja, N. and Raj, M., 2013. Proprietary software versus Open Source Software for Education. American Journal of Engineering Research (AJER), [online] 02(07), p.126. Available at: https://www.ajer.org/papers/v2(7)/O027124130.pdf [Accessed 18 December 2021].

Jackson, S. and Brannon, S., 2018. In-house Software Development: Considerations for Implementation. The Journal of Academic Librarianship, 44(6), pp.689-691.

Campbell, T., 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation. 1st ed. Springer Nature.

Crumbley D L, Heitger L E and Smith G S 2007. Forensic and Investigative Accounting, 3rd Edition, Commerce Clearing House, Chicago, IL.

Hadnagy, C.,2018. Social Engineering: The Science of Human Hacking. 2nd ed. Indianapolis: Wiley.

Sutton, D. (2014), Information Risk Management, Ingram Publisher Services UK- Academic, [Insert City of Publication]. Available from: VitalSource.

Brody, R. and Kearns, G., 2009. IT Audit Approaches for Enterprise Resource Planning Systems. The Icfai University Journal of Audit Practice, 6(2).

FIRST — Forum of Incident Response and Security Teams. 2021. CVSS v3.1 Specification Document. [online] Available at: <https://www.first.org/cvss/specification-document#1-2-Scoring> [Accessed 18 December 2021].

Houmb, S., Franqueira, V. and Engum, E., 2009. Quantifying security risk level from CVSS estimates of frequency and impact. The Journal of Systems and Software,.

Rodriguez, C. and Gürcay, O., 2020. Open-Source Software in Business and its Advantages & Disadvantages.