**Risk Assessment Report for ACM**

Small Medium Enterprises (SMEs) face many issues, such as selecting the best technology to support operations and cyber security threats. It is usual for SMEs to choose a series of faulty IT systems that become outdated and inefficient with time. Besides, limited access to capital, low research and development expenditure, and lack of technical experts can make them struggle to create a secure environment where new systems seamlessly integrate with others (Thompson et al., 2012). The need for an ACM manufacturing company to acquire an ERP (Enterprise Resource Planning) solution to respond to market dynamics also pauses challenges to the business. Therefore, this report analyzes the risks associated with the ERP solution based on the NIST framework to provide a cost-benefit analysis and disaster recovery plan for the company.



**Figure 1.1 *Selected Framework***

The framework was created with an emphasis on sectors crucial to economic and national security, such as the military industrial base, banking, energy, and finance.

1. (NIST 800-53 - The NIST) Cybersecurity framework was developed to respond to the presidential Executive.

2.(ISO 27K - The ISO 27001) Cybersecurity framework consists of international standards which recommend the requirements for managing (ISMS) information security management systems.

3. COBIT (Control Objectives Business’s Information Technologies) Cybersecurity framework that incorporates the greatest elements of IT security for a company.

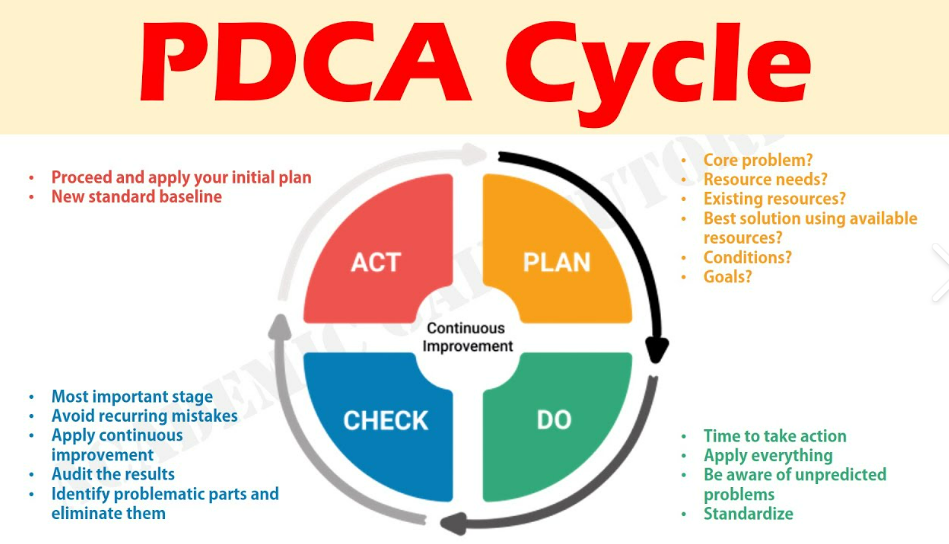
The National Institute of Science and Technology (NIST) is the preferred framework for analyzing ACM's risks. It is a well-regarded framework for information security and cyber risk management because it provides easy-to-understand risk management solutions for 16 critical sectors of critical infrastructure (Alshboul & Streff, 2015, p. 1; Paulsen & Toth, 2016, p. 4).

·       NIST was created to accommodate all entities because small and mid-sized businesses may have budget and staff constraints to manage risks. Therefore, its simplicity and reality prove valuable even for smaller companies.

·       Its well-taxonomy called CSF score (identify, protect, detect, respond, recover) makes cybersecurity management for non-experts convenient and easy to understand. Therefore, executives can focus on the five levels of the CSF score to understand their security posture at a higher level.

·       Overall, the layered taxonomy of the NIST framework allows for flexible cybersecurity awareness communication at all levels, from the ICT department to the board members. The business can adopt whatever level is needed to meet its customized needs with the NIST (Paulsen & Toth, 2016). You can start with a subset of the categories, subcategories, and controls, then expand over time.

**PDCA (PLAN DO CHECK ACT)**



**To use the PDCA cycle:**

1. Launching a new renovation project.
2. Designing a process, a product, or a service with a new or enhanced layout.
3. A repetitive work process definition.
4. Organizing data collecting and analysis to confirm and rank issues or their primary causes.
5. Putting any change in place.
6. Aiming for ongoing progress.

**Risk Analysis**

**Table 1**: Risk Analysis Approach and Justification

|  |  |  |
| --- | --- | --- |
| **Risk** | **Analysis Approach** | **Justification** |
| Lack of formalized decision-making process | Qualitative | There is no approximate way to estimate whether decisions made by the business will succeed or not because that is dependent on several factors, such as the market and economy. Therefore, the analysis approach is qualitative because the risk tends to be more subjective. |
| Lack of business continuity plan | Qualitative | The cost of business interruption varies due to several events that may or may not occur. Since the outcome is unknown in advance, its consequences can only be measured using qualitative analysis. |
| Cybersecurity threats | Qualitative | Qualitative risk assessment is applicable since cybersecurity threats are uncertain events, but their outcome can have severe consequences for the business. For instance, the impact and cost of consequences like downtime, loss of productivity, and trust can only be estimated. |
| High cost of acquiring ERP | Quantitative | The quantitative approach is applicable here because the cost of acquiring an ERP solution is known, including the financial position of the business to purchase the software. |
| Incompatibility with the existing solution | Qualitative | The ERP's inability to operate satisfactorily with other systems is an uncertain event that could have many outcomes. Therefore, its likelihood is best measured using a qualitative approach. |
| ERP complexity for users and support | Qualitative | User acceptance and ability to learn the new system are subjective and can only be determined after deploying the ERP system. |

**Table 2**: Risk Weight, where PI score represents Low (1-3), Medium (4-6), and High (7-9)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Probability (1-3)** | **Impact (1-3)** | **PI Score** | **Risk Response Type** |
| Lack of formalized decision-making process | 2 | 2 | 4 | Avoided |
| Lack of business continuity plan | 1 | 3 | 3 | Avoided |
| Cybersecurity threats | 2 | 3 | 6 | Reduced |
| High cost of acquiring ERP | 2 | 2 | 4 | Transferred |
| Incompatibility with the existing solution | 2 | 2 | 4 | Shared |
| ERP complexity for users and support | 3 | 1 | 3 | Retained |

**Cost-Benefit Analysis**

**Table 3**: Risks and their mitigation withe associated cost of mitigating threat impact

|  |  |  |
| --- | --- | --- |
| **Risk** | **Mitigation** | **Cost** |
| Lack of formalized decision-making process | ·   Integrate information security governance activities with the overall organization structure. They include establishing roles and responsibilities, integrating with the enterprise architecture, strategic planning, and documentation of security objectives (Pauline Bowen et al., 2006, p. 2).  ·   Ensure appropriate participation of the business officials in overseeing the implementation of information security controls throughout the business (Pauline Bowen et al., 2006, p. 2). | $850 |
| Lack of business continuity plan | ·   Periodically assess risks and magnitude resulting from disruption, unauthorised access, and destruction of information and information systems.  ·   Develop risk-based and cost-effective information security policies, control techniques, and procedures to address applicable threats (Pauline Bowen et al., 2006, p. 10). | $1200 |
| Cybersecurity threats | ·   Implement network and user-level security controls, such as firewalls, antivirus programs, and user access controls (Pauline Bowen et al., 2006, p. 12).  ·   Regularly conduct a risk assessment to determine vulnerabilities.  ·   Build an incident response plan | $3200 |
| High cost of acquiring ERP | ·   Select appropriate ERP based on business needs by focusing on long-term return on investment.  ·   Select the right implementation plan for the business by considering hosting on the cloud. | $4500 |
| Incompatibility with the existing solution | ·   Outsource the ERP solution from credible vendors with experienced experts in ERP deployment, integration, and configuration.  ·   Consider moving the ERP software to the cloud, where a vendor can maintain it. | $300 |
| ERP complexity for users and support | ·   Provide training and share the information with employees who will interact with the ERP.  ·   Use visual materials to help improve technology acceptance. | $860 |
| **Total** | **Note**: The total cost of mitigating risks associated with the new ERP solution | $10910 |

The main emphasis of the cost-benefit analysis is the trade-off between paying to prevent the risks versus paying to clean up after an incident. Notably, the cost ACM will incur for acquiring the new ERP solution, including mitigation expenses, is valued at $10,910. According to a Sophos survey in 2021, the average cost of recovery from a ransomware attack increased from $761,106 in 2020 to $1.85 million in 2021 (Atkin, 2021, pp 12). Therefore, it is clear the preventive cost prevails compared to the cost of a breach.

**Disaster Recovery Items**

**Table 4**: Allocated RTO values for the risks, justification, and implication of the RTO on the company

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **RTO/RPO** | **Justification** | **Implications to the Company** |
| Network equipment, e.g., routers | RTO: 30 minutes | Network equipment failure can prevent workers from accessing ERP systems and cloud data. | Access to the ERP system will be unavailable for 30 minutes, resulting in a loss of productivity. |
| Telecommunication services, e.g., Internet service provider | RTO: 1 Hour | Employees can use modems to access the internet when the service provider is offline for a maximum of 1 hour. | The company incurs an additional cost on internet access, including slow connectivity. |
| Computing hardware, e.g., servers, desktop computers, laptops, and operating system | RTO: 6 Hours | Employees can use alternative desktops/servers/laptops if one or more are being repaired. | Loss of productivity if alternative computing hardware is not available |
| Power | RTO: 10 Minutes | Backup power generators and uninterruptible power supply should go on to support critical systems. | Power outage beyond 10 minutes will cripple all operations and cause customer service interruptions |
| Cloud service providers, e.g., ERP hosting and data backup vendors | RTO: 30 Seconds | The ERP will be inaccessible to employees and customers | All operations requiring access to ERP will be interrupted, causing productivity and financial losses. |

**Figure 1.2**: The proposed solution is a cloud-based ERP.

**Proposed Solution**

***Challenges Addressed by the Solution***

·       **Resilience**: the solutions take advantage of redundancy offered in the cloud, eliminating a single point of hardware failure. Software-as-a-Service (SaaS) ERPs are also less susceptible to hardware failure. Also, the backup Internet carrier enables the business to continue accessing the cloud ERP if the other fails.

·       **Network security**: the firewall validates access to the internal systems by assessing incoming traffic for anything malicious. The cloud environment also has robust security protocols and features to prevent possible intrusion or attack.

·       **Vendor lock-in**: the ERP is built as a portable application with the flexibility to be implemented on various platforms and operating systems without major modification to the code.

**Conclusion**

​To sum up, the report has provided a comprehensive analysis of the critical risks facing Acme Manufacturing Company. It has recommended the use of a backup plan strategy to mitigate the risks and avoid them in the future. Further, the study has applied qualitative and quantitative approaches to analyze the risks to develop an effective solution. Therefore, if the solution is applied profoundly, the firm will gain a competitive advantage and boost its performance and productivity.

# **References**

Alshboul, Y. & Streff, K., 2015. *Analysing Information Security Model for Small-Medium Sized Businesses.* Puerto Rico, 21st Americas Conference on Information Systems.

Atkin, P., 2021. *Adopting a cost-benefit analysis approach to cybersecurity.* [Online] Available at:https://www.itproportal.com/features/adopting-a-cost-benefit-analysis-approach-to-cybersecurity/ [Accessed 23th of July 2022].

Pauline Bowen, Hash , J. & Wilson, M., 2006. *Information Security Handbook: A Guide for Managers,* s.l.: NIST.

Paulsen, C. & Toth, P., 2016. *Small Business Information Security: The Fundamentals,* s.l.: National Institute of Standards and Technology.

Thompson, C., Bounds, M. & Goldman, G., 2012. THE STATUS OF STRATEGIC PLANNING IN SMALL AND MEDIUM ENTERPRISES: PRIORITY OR   AFTERTHOUGHT? *SAJESBM Volume,* 5(127), pp. 34-53.

https://www.bing.com/images/search?view=detailV2&ccid=ZBDRc4wd&id=90BBBA29AAE26E69C953EE6E3FCBC4F09B67E42F&thid=OIP.ZBDRc4wdhDmB9hGzk2psxAHaEK&mediaurl=https%3a%2f%2fi.ytimg.com%2fvi%2fyQRCwJnRU80%2fmaxresdefault.jpg&cdnurl=https%3a%2f%2fth.bing.com%2fth%2fid%2fR.6410d1738c1d843981f611b3936a6cc4%3frik%3dL%252bRnm%252fDEyz9u7g%26pid%3dImgRaw%26r%3d0&exph=720&expw=1280&q=Vidoes+Explaining+PDCA+Cycle&simid=608014610418905100&FORM=IRPRST&ck=13A1C113189F95CCE1D35FEF686C1D84&selectedIndex=0&ajaxhist=0&ajaxserp=0 [Accessed 23th of July 2022].

https://cyberexperts.com/cybersecurity-frameworks/#:~:text=%2023%20Top%20Cybersecurity%20Frameworks%20%201%20ISO,standards%20designed%20to%20enable%20small%20and...%20More%20 [Accessed 23th of July 2022].

https://www.mindtools.com/pages/article/newPPM\_89.htm [Accessed 23th of July 2022].