RISK ASSESSMENT

NIST Framework

A corporate risk management program must include adopting a risk management approach. With cyber-threats expected to cost the globe $6 trillion per year by 2021 (Williams et al, 2020), businesses must choose the finest and most effective risk assessment technique to manage their risks.

There are several risk assessment frameworks such as Open Fair, ISO, NIST etc. that are effective in performing a risk analysis. The NIST Cybersecurity Framework is a risk assessment approach that aids enterprises in providing a rigorous risk assessment program (Gillis, 2021). It is one of the primary international references in IT risk management. It is ideal for this risk assessment since it:

* Ensures organizations adhere to industry standards.
* Analyzes cyber hazards to lay the groundwork for a cybersecurity plan.
* Evaluates the efficacy of IT security policies.
* Determines the probable severity of the risks to which the ACME is exposed.
* Enhances cybersecurity breach handling procedure.
* Improves cybersecurity communication with stakeholders.

The NIST Framework is made up of three primary parts, which include:  the Profile,  Core, and Tiers.

Graph 1: NIST CSF main components (Keller, 2018)

* The core of the framework is a collection of actions and network security outcomes that includes functional functions, categories, and subcategories with a high function level of five. See Table 1 for further information. Five functions apply not just to network safety risk management, but also to risk management in general.

|  |  |  |
| --- | --- | --- |
| **Functions** | **Category** | **ID** |
| **Identify** | Asset Management | ID.AM |
| Business Environment | ID.BE |
| Governance | ID.GV |
| Risk Assessment | ID.RA |
| Risk Management Strategy | ID.RM |
| Supply Chain Risk Management | ID.SC |
| **Protect** | Identity Management and Access Control | PR.AC |
| Awareness and Training | PR.AT |
| Data Security | PR.DS |
| Information Protection Processes & Procedures | PR.IP |
| Maintenance | PR.MA |
| Protective Technology | PR.PT |
| **Detect** | Anomalies and Events | DE.AE |
| Security Continuous Monitoring | DE.CM |
| Detection Processes | DE.DP |
| **Respond** | Response Planning | RS.RP |
| Communications | RS.CO |
| Analysis | RS.AN |
| Mitigation | RS.MI |
| Improvements | RS.IM |
| **Recover** | Recovery Planning | RC.RP |
| Improvements | RC.IM |
| Communications | RC.CO |

Table 1: NIST CSF Core. (Keller, 2018)

* The execution levels vary from partial (level 1) to adaption (level 4) and define the severity of the well-understood evolution of network risk decisions. Larger risks are rated and measured when an organization shares and gets information about the network security of external elements.
* Records are a one-of-a-kind link between companies and their goals, as measured by hunger and resources vs the frame core's intended outcomes. By comparing the present profile to the goal profile, they may find areas for cybersecurity improvement

Risk Analysis

1. COTS Solution

Scenario: Unauthorized access to ACME network due to the introduction of the new COTS system.

Approach: To identify gaps, qualitative risk analysis was done by conducting interviews with SMEs stakeholders. The below weaknesses were determined as a result of the interviews.

Asset: COTS software

Threat and vulnerability Description

* Unauthorized access to the COTS system through the Internet to evade or undermine it.
* Existing or undiscovered vulnerabilities in the COTS system might be used to compromise the internal customer network.
* A COTS solution with a compromised server might be used to establish contact with internal systems.
* A misconfiguration of the COTS system might allow unauthorized access to unapproved services, potentially resulting in data leakage.

Weaknesses

* The solution code is a closed-loop system that is difficult to secure.
* The solution's components are very likely to be insecure and exploitable.
* The absence of qualified staff will obstruct the resolution of security concerns that have been raised.
* Without a solution, ACME will be vulnerable to Denial-of-Service assaults.
* The solution will be vulnerable to web application assaults due to the lack of a web application firewall.

Risk Evaluation

Below is the overall risk rating (High) based on the currently mentioned weaknesses.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood Rating: (Probability of single occurrence in one, three or ten years)  The introduction of the COTS solution increases the likelihood of a compromise. | | | | | | | | | | | | | |
| Very low (1) | | | Low (2) | | | Medium (3) | | | High (4) | | | Very High (5) | |
| Impact Rating based on Impact Matrix:  Financial, Reputation, Strategy Achievement, Compliance, Business Interruption, Health and Safety, Security.  The introduction of a COTS solution will increase the risk factors which may lead to a compromise of the customer systems. | | | | | | | | | | | | | |
| 1 | 2 | | 3 | 4 | | 5 | | 6 | 7 | | 8 | | |
| Overall rating: | | | | | | | | | | | | | |
| A | | B | | | C | | D | | | E | | | F |

Recommendations:

* Conduct a full security assessment of the solution, including penetration testing. It will help ACME determine vulnerabilities in the software and patch them up before hackers gain access to the system.
* Ensure that connectivity to external cloud services is validated, managed, and monitored.
* Protect the solution from DoS attacks by using a Denial of Service (DoS) solution or service.
* To protect against online application attacks, set up a web application firewall. It will help block out any unauthorized access to the system and act as an alerting service to notify security analysts that an intrusion is about to happen.
* Check that the solution's configurations match the security configuration baseline (SCB) for the business system.

Below is the overall risk rating (Low) after implementing the recommended controls.

Risk treatment: Risks should be accepted, and recommended controls implemented to mitigate them.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood Rating: (Probability of single occurrence in one, three or ten years)  The introduction of the COTS solution increases the likelihood of a compromise. | | | | | | | | | | | | | | | |
| Very low (1) | | | Low (2) | | | | Medium (3) | | High (4) | | | | Very High (5) | | |
| Impact Rating based on Impact Matrix:  Financial, Reputation, Strategy Achievement, Compliance, Business Interruption, Health and Safety, Security.  The implementation of the recommended controls will significantly decrease the risk factors which may lead to a compromise of ACME systems. | | | | | | | | | | | | | | | |
| 1 | 2 | | | 3 | | 4 | | 5 | | 6 | | 7 | | | 8 |
| Overall rating: | | | | | | | | | | | | | | | |
| A | | B | | | C | | | D | | | E | | | F | |

1. Open-source

Scenario: Untrusted Open-source software installation may lead to unauthorized access to ACME critical systems and confidential data.

Approach: Qualitative risk analysis was used by conducting interviews with stakeholders SMEs to identify existing gaps. The below weaknesses were determined as a result of the interviews.

Asset: Open-source software

Threat and vulnerability Description

* The solution can be accessed without authorization if there is no software support.
* The Blackhat community may have already hacked and modified the solution, placing it in danger.
* Publicly known or unreported vulnerabilities may be exploited to access the solution and damage the business.
* Due to a lack of formal security improvements including zero-day vulnerabilities in the solution might leave it vulnerable to attacks and exploits indefinitely.
* The existence of backdoors may not be found even after a comprehensive and extensive security evaluation.

Weaknesses

* The software version does not have all the security recommendations implemented due to a lack of support.
* The selected software version source availability to the Blackhat community will leave the business open to compromises.
* No formal mechanism is available to update the software. Security updates are released ad hoc and will not necessarily remediate reported security issues.
* There are no resources to check for available zero-day vulnerabilities.
* There are no available resources to check for possible backdoors.
* Lack of Denial-of-Service solution to protect against denial of service attacks.
* Lack of a web application firewall to protect from web application attacks.

Risk Evaluation

Below is the overall risk rating (Very High) based on the currently mentioned weaknesses.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood Rating: (Probability of single occurrence in one, three or ten years)  The introduction of the Open source ERM solution greatly increases the likelihood of a compromise. | | | | | | | | | | | | | |
| Very low (1) | | | Low (2) | | | Medium (3) | | | High (4) | | | Very High (5) | |
| Impact Rating based on Impact Matrix:  Financial, Reputation, Strategy Achievement, Compliance, Business Interruption, Health and Safety, Security.  The introduction of an open source solution will significantly increase the risk factors, which will lead to a compromise of ACME systems. | | | | | | | | | | | | | |
| 1 | 2 | | 3 | 4 | | 5 | | 6 | 7 | | 8 | | |
| Overall rating: | | | | | | | | | | | | | |
| A | | B | | | C | | D | | | E | | | F |

Recommendations:

* Conduct a complete and comprehensive security assessment, including penetration testing of the system.
* Develop a formal patch management process to ensure regular updates of the software. Updating the software will help eliminate the vulnerabilities in the system or the probability of a backdoor.
* Assess and remediate issues identified in the various compromise reports of the solution.
* Deploy or engage the service of a third-party DDoS provider to protect the solution from Denial of service (DoS) attacks.
* Deploy a web application firewall to protect the solution from web application attacks. It ensures that hackers cannot gain entry into ACME servers or networks through the software.
* Verify the configurations of the solution and ensure they are in alignment with the
* is business system security configuration baseline (SCB).

Below the overall risk rating (High) after implementing the recommended controls.

Risk treatment: Risks should be avoided, as recommended controls will not fully mitigate the risks even if they are fully implemented.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood Rating: (Probability of single occurrence in one, three or ten years)  The introduction of the COTS solution increases the likelihood of a compromise | | | | | | | | | | | | | | | |
| Very low (1) | | | Low (2) | | | | Medium (3) | | High (4) | | | | Very High (5) | | |
| Impact Rating based on Impact Matrix:  Financial, Reputation, Strategy Achievement, Compliance, Business Interruption, Health and Safety, Security.  The implementation of the recommended controls will not decrease the risk factors, which will lead to a compromise of ACME systems and data. | | | | | | | | | | | | | | | |
| 1 | 2 | | | 3 | | 4 | | 5 | | 6 | | 7 | | | 8 |
| Overall rating: | | | | | | | | | | | | | | | |
| A | | B | | | C | | | D | | | E | | | F | |

1. In House

Scenario: Potentially unsecure CRM solution with access to internal computing resources and data may lead to exposure of company data.

Approach: Qualitative risk analysis was used by conducting interviews with stakeholders SMEs to identify existing gaps. The weaknesses below were determined due to the interviews and validating of SMEs' inputs.

Asset: In House CRM software

Threat and vulnerability Description

* A non-existent support model for the solution may prevent the company from reaching its goals.
* The lack of regular updates and testing may expose the solution to severe operations and security issues.
* Code failure may significantly affect the business and cause a significant operational impact.
* The lack of dependency matrix of the solution may not provide complete visibility on what may be affected if the solution is breached.
* The lack of a DevSecOps framework may reduce the company's security posture.

Weaknesses

* A lack of support model will lead to the solution being out of operation in the event of a code failure.
* Lack of dependency matrix that shows all possible affected business processes and systems.
* Lack of application of the DevSecOps framework during the development process.
* Lack of Denial-of-Service solution to protect against denial of service attacks.
* Lack of a web application firewall to protect against web application attacks.

Risk Evaluation

Below is the overall risk rating (High) based on the currently mentioned weaknesses.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood Rating: (Probability of single occurrence in one, three or ten years)  The introduction of the Open source ERM solution greatly increases the likelihood of a compromise. | | | | | | | | | | | | | |
| Very low (1) | | | Low (2) | | | Medium (3) | | | High (4) | | | Very High (5) | |
| Impact Rating based on Impact Matrix:  Financial, Reputation, Strategy Achievement, Compliance, Business Interruption, Health and Safety, Security.  The introduction of an in house developed solution will significantly increase the risk factors, which may lead to a compromise of the customer systems. | | | | | | | | | | | | | |
| 1 | 2 | | 3 | 4 | | 5 | | 6 | 7 | | 8 | | |
| Overall rating: | | | | | | | | | | | | | |
| A | | B | | | C | | D | | | E | | | F |

Recommendations:

* Conduct a complete and comprehensive security assessment, including penetration testing of the solution.
* Develop a formal patch management process to ensure the update of the software. Updating the software will help eliminate the vulnerabilities in the system or the probability of a backdoor.
* Develop a formal support process to ensure issues to the code are remediated.
* Ensure the DevSecOps framework is followed and implemented.
* Develop a dependency matrix of all business processes and systems. The matrix will help ensure that each person has the correct permissions based on the nature of the job at ACME.
* Implement a solution for protection from Denial of service (DoS) attacks.
* Deploy a web application firewall to protect the solution from web application attacks.
* Verify the configurations of the solution and ensure they are in alignment with the company system security configuration baseline (SCB).

Below is the overall risk rating (Medium) after implementing the recommended controls.

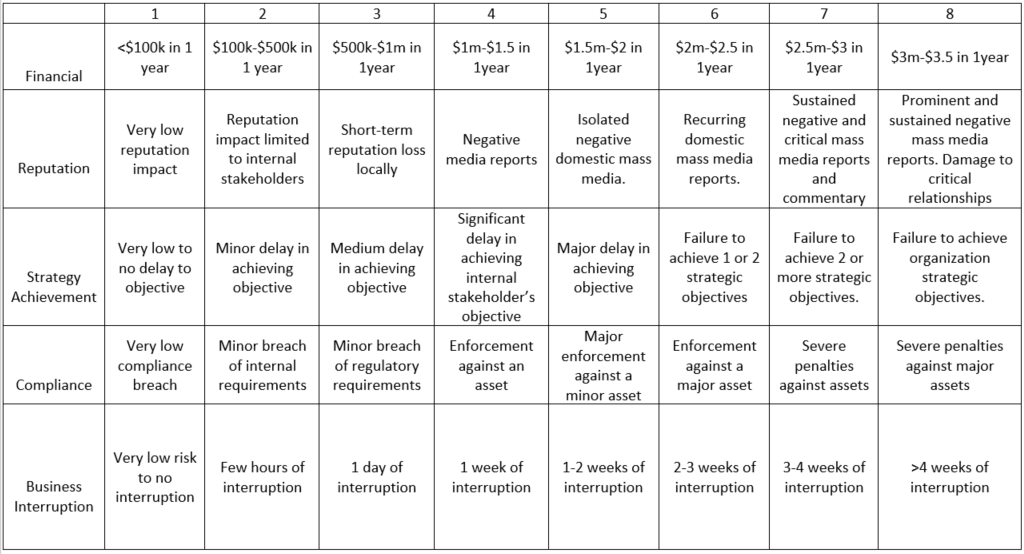
Risk treatment: Risks should be transferred, and recommended controls implemented as possible.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood Rating: (Probability of single occurrence in one, three or ten years)  The introduction of the COTS solution increases the likelihood of a compromise | | | | | | | | | | | | | | | |
| Very low (1) | | | Low (2) | | | | Medium (3) | | High (4) | | | | Very High (5) | | |
| Impact Rating based on Impact Matrix:  Financial, Reputation, Strategy Achievement, Compliance, Business Interruption, Health and Safety, Security.  The introduction of a COTS solution will significantly increase the risk factors, which may lead to a compromise of the customer systems. | | | | | | | | | | | | | | | |
| 1 | 2 | | | 3 | | 4 | | 5 | | 6 | | 7 | | | 8 |
| Overall rating: | | | | | | | | | | | | | | | |
| A | | B | | | C | | | D | | | E | | | F | |

Risk Acceptance Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Likelihood calculation | 1 yr | 3 yrs | 10 yrs |
| Very High | >25% | >60% | >95% |
| High | 10-25% | 25-60% | 65-95% |
| Medium | 5-10% | 15-25% | 40-65% |
| Low | 1-5% | 3-15% | 10-40% |
| Very Low | <1% | <3% | <10% |

|  |  |
| --- | --- |
| Severity | Prioritization of Actions |
| A | To be dealt with as an urgent business priority |
| B | To be dealt with as a business priority |
| C |
| D | To be dealt with in accordance with the operating plan of the designated risk owner. |
| E |
| F | To be dealt with as deemed necessary by the designated risk owner. |



Disaster recovery plan

A Disaster Recovery Plan (DRP), for the IT sector is a written policy and procedure used to assist an organization in implementing disaster recovery procedures in order to protect the company's IT infrastructure and promote overall recovery (Druva,2021). The purpose of ACME's disaster recovery plan is to spell out the procedures that must be followed before, during, and after a natural or fabricated disaster so that everyone on the team can follow them. A disaster recovery plan must manage both intentional and inadvertent manufactured disasters, such as the aftermath of a terrorist strike or attack, as well as unintentional disasters, such as equipment failure (Druva, 2021). The first step is to determine the decision based on the risk analysis conducted above.

Decision

The COTS CRM solution is the suggested option for ACME based on the risk analysis completed on the three solutions and specific weaknesses and dependent on the suggestions being implemented and confirmed (ResQSoft, 2012). This will assist ACME in reducing the chance of danger to a bare minimum. The benefit of a COTS solution is that it assures ACME utilizes the appropriate software for its purposes. Because the program is tiny, there are few to no weaknesses, and there are no issues such as backdoors that would allow hackers to enter the system (ResQSoft, 2012) quickly. Some solutions and recommendations apply to all three methods, addressing numerous flaws and vulnerabilities. A standard guideline for all three, for example, is to continually monitor systems to verify that they are in excellent working order. As a result, there was an issue with continuous system testing and monitoring.

The reason for choosing COTS is that Custom software is usually more costly than COTS software. Another factor to consider is that commercial software is often quite dependable. The most frequent sorts of business processes or problem-solving strategies are studied by COTS component developers and packaged into software packages that may be utilized at any level (ResQSoft, 2012). Another advantage for ACME to use COTS products is that besides the easy integration and installation of the systems, they also have customer care, which is a plus for the company.

In case there is a problem with the COTS products, there are fixes and patches that are readily available. These fixes imply that they could create vulnerabilities for ACME. Such vulnerabilities could include hacking and enabling easy access to sensitive data by hackers. Besides, when ACME decides to customize these COTS products, it could become expensive for them compared to purchasing customized products.

Solution

To help prevent the vulnerabilities and risks determined from the COTS system affecting ACME Company, the Trust Enhancing (TE) architecture should be used. The solution system is split and specified into several functional domains in TE architecture (Tucker, 2015). Cybersecurity technologies are used in each of these functional domains. Each functional area has nine main features that give it its perspective on the system or subsystem security: system monitoring, software security, upgrades and patches, configurations, and forensics (Tucker, 2015). These features are essential because they help determine and reduce the COTS products' vulnerabilities for ACME.

The TE architecture employs a Container/Security Enclave, which is built using an object-oriented design technique that incorporates the following design criteria:

* Physically isolating the COTS software from the critical environments.
* Implementing the use of advanced firewalls that also monitor and detect intrusions.
* Hide all processes from external viewing, which could be exploited (Tucker, 2015).
* Continuous testing of the system.
* Installation of a model with the least privilege to help limit personal access.
* Help with control and management of the system and the upgrades and patches (Tucker, 2015).

This technique allows for file integrity, monitoring service usage/user profiles, providing automatic security measures, and managing and monitoring settings (Tucker, 2015). The architecture is as shown below:

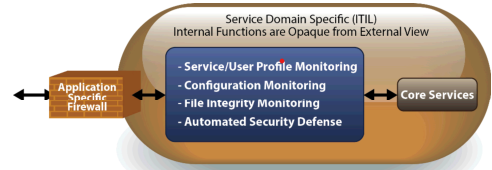


Figure 1: Security Container used by TE architecture (Tucker, 2015: 4)

Importance of the TE solution

The least privileged security model in the TE architecture begins by entirely shutting down the system and progressively enables accessibility or communication to the required degree of functionality, but no more (Tucker, 2015). This necessitates a thorough understanding of the current software environment, data exchange across services, typical user behavior, and network traffic.

The focus is on the people, technology, and operations domains since the TE architecture is built on the protection, detection, and reaction paradigm. If not, all areas are covered, and due diligence ensures an adequate plan has not been performed (Tucker, 2015). Policies and procedures, training, physical security, and personnel security must be handled in the people sector. A specified patching process, system security assessment, system monitoring, attack response methods, and backup and recovery should be handled in the operational domain. The proposed TE architecture employs outer perimeter protection to defend against Internet threats at the application and network layers. These protectors filter traffic in and out of the TE Architecture industry on specific ports (Tucker, 2015). They also provide a primary point of contact for the organization's security operations center (SOC), where security analysts may monitor threats and provide user authentication services, SSL blocking, and content filtering.

A monitoring/application layer follows the network layer. This particular element has several tools for monitoring network traffic, both encrypted and unencrypted, to gain a complete picture of what is going on in the TE Framework (Zheng & Oleshchuk, 2011). The monitoring software will be developed to acquire insight and evaluate user behavior, and COTS software will generate a profile. The area's in-depth protection is enhanced by this monitoring software paired with an authoritarian operating system and limited space. In addition to monitoring software, the TE Framework may be simply linked with network monitoring technologies presently in use by businesses (Yuan et al., 2019).

Beyond the organizations present security rules and processes, there are several items to consider once a system is online. The development of policies and processes concerning container security and the deployment of a trusted software process are two topics of importance in the TE framework (Tucker2015). The TE architecture suggests that policies and processes be implemented to limit access to computers in certain zones. According to this policy, any administrative access to the surrounding territory must go through a central location. Instead of allowing open access, this single access point should be set up such that users only have limited access to the computers they require (Tucker, 2015). The TE architecture will also ensure that the patches and upgrades to the COTS software are secure and will not introduce vulnerabilities to the system.

References:

Druva. (2012) Disaster Recovery Plan. Avaliable from: <https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs/> [Accessed 6 April 2022].

Gillis, Alexander S. (2021) NIST Cybersecurity Framework. Avaliable from: <https://www.techtarget.com/searchsecurity/definition/NIST-Cybersecurity-Framework> [Accessed 4 April 2022].

Keller, N. (2018) An Introduction to the Components of the Framework. Available from: <https://www.nist.gov/cyberframework/online-learning/components-framework> [Accessed 4 April 2022].

Mesker, K. (2014) Adapting NIST Cybersecurity Framework for Risk Assessment. Available at: https://www.nist.gov/system/files/documents/cyberframework/cybersecurityframework\_6thworkshop\_chevron.pdf [Accessed 5 April 2022].

ResQSoft. (2012) The Basics of COTS – Commercial-Off-The-Shelf Software. Avaliable from: <https://www.resqsoft.com/basics-cots-%E2%80%93-commercial-off-the-shelf-software.html> [Accessed 3 April 2022].

Tucker, M. (2015) TE Framework: A Framework for Securing COTs Applications. Avaliable from: <https://www.osti.gov/servlets/purl/1332894> [Accessed 5 April 2022].

Williams, C.M., Chaturvedi, R., Chakravarthy, K. (2020) Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research* 22(9): 1-4. DOI: [10.2196/23692](https://dx.doi.org/10.2196%2F23692)

Yuan, Z. et al. (2019) *B2SFinder: detecting open-source software reuse in COTS software*. Avaliable from: <https://dl.acm.org/doi/10.1109/ASE.2019.00100> [Accessed 4 April 2022]

Zheng, X & Oleshchuk, V. (2011) Trust enhancement of P2PSIP communication systems.  *Journal of Internet Technology and Secured Transactions* 3(2): 121 -131. Avaliable from: <https://www.inderscienceonline.com/doi/abs/10.1504/IJITST.2011.039773> [Accessed 5 April 2022].