The importance of a risk register as a decision aid is that it helps an organization analyze the risks, monitor and control, and plan responses accordingly to help mitigate the risks (Usmani, 2022). Also, a risk register helps provide a number representing the probability of impact and occurrence. From previous work in this class that number has been between one and three. One represents the lowest impact and occurrence, while three represents the highest impact and occurrence. The relationship between a risk register and a threat landscape is that the threat landscape helps protect an organization from known threats and regular everyday threats every organization faces. A risk register helps protect an organization by identifying potential threats that could threaten an organization. The risk register must identify these potential threats to send into the threat landscape to help protect the organization.

Business impact analysis helps in decision aid by providing the organization with what processes are most crucial to keep running for the organization (Alonso, 2020). This is done by analyzing business processes to know what impact occurs in the event of a threat that causes this process to stop running (Alonso, 2020). The relationship between business impact analysis and survivability of an organization helps keep the business afloat in a crisis. The organization can organize the processes' impact and have procedures in place in case of failure. This is a way to help mitigate the impact of a threat and allow the organization to keep the business running. If an organization server shuts down it will disconnect customers from their website, which is a vital process for the company. The BIA recognizes that, and the organization understands for their company to survive they must have a backup server in the event of the first server going down, because of the impact it would have on the company.

System’s thinking mindset helps troubleshoot problems by not causing unintended consequences (Lethbridge College, 2021). This is done by understanding what change to a system can cause a change to another system and so on. An organization’s system is often overlapping which is why all employees should understand the complexity of how each system is connected so when providing a solution, it does not make the situation worse. Instead, when an employee provides a solution, it should work for the entire system, provide a complete solution, and correct the problem (Lethbridge College, 2021).

The value of understanding the adversary mindset is that an organization can know what the actor is targeting and why, which can help the cyber defense team prevent the most threatening adversaries from attacking (Nace, 2021). Also, understanding the adversary better can help the defense team not make guesses to the number of threats they have but instead make educational decisions in advance to an attack to deter the threat actor from penetrating the organizations system in the first place (Nace, 2021).

The value of confidentiality for security risk management planning is securing information like Personal Identifiable Information (PII) from threat actors. This protects the customer's information from being misused and protects the organization also from being sued for illegal access. Confidentiality is important also to prevent information like customer's activities and financial information from companies like Google, Apple, and Amazon (Henderson, 2015). This is done by making sure channels are properly secured by being monitored and controlled to prevent unauthorized access (Henderson, 2015).

The value of integrity for security risk management planning is to make sure financial information is not changed. This provides the customers with confidence that the company values consistency, accuracy, and value of their information (Henderson, 2015). According to (Henderson, 2015) Integrity aids in decision making and helps to meet integrity objectives.

The value of availability for security risk management planning is to make sure information is released to be available to the public. For a secure risk management plan there should be minimal downtime for websites and systems. Governments ensure that there are insignificant downtimes for websites and systems, as they will use backups if they need to, to ensure that public information is available (Henderson, 2015). The value of the CIA (Confidentiality, Integrity, and Availability) triad is to protect valuable information from unauthorized access, stop modification and disruption to systems. The CIA triad according to (Henderson, 2015) ensures success by guiding information security efforts for confidentiality, integrity, and availability which are basic factors in information security.

**References**

Usmani, F. (2022, October 24). *What is Risk Register? Definition with Example. |*. PM Study Circle. [https://pmstudycircle.com/risk-register/#:~:text=A%20risk%20register%20provides%20all%20information%20on%20project](https://pmstudycircle.com/risk-register/)

Nace, M. (2021, September 4). *Leading the way with an adversary focus*. Deloitte Insights. <https://www2.deloitte.com/us/en/insights/industry/public-sector/government-deter-cybersecurity-adversary.html>

Henderson, A. (2015, July 5). *The CIA Triad: Confidentiality, Integrity, Availability*. Panmore Institute. [https://panmore.com/the-cia-triad-confidentiality-integrity-availability#:~:text=The%20CIA%20triad%20has%20the%20goals%20of%20confidentiality%2C](https://panmore.com/the-cia-triad-confidentiality-integrity-availability)

Lethbridge College. (2021, December 4). *The Value of a Systems Thinking Mindset*. Learning Innovation | Centre for Teaching, Learning and Innovation | Lethbridge College. <https://learninginnovation.ca/the-value-of-a-systems-thinking-mindset/>

Alonso, C. (2020, May 22). *What is BIA? What is its importance in Business Continuity?* GlobalSUITE Solutions. <https://www.globalsuitesolutions.com/what-is-bia-what-is-its-importance-in-business-continuity/>