Topic 8 Discussion 2

There are many ways to go about assessing the overall framework and structure of a secure information environment. Research and discuss how an organization can assess its cybersecurity programs. Should there be a regulatory requirement for organizations to have an external audit?

Hello Class,

Organizations can assess their cybersecurity programs through a variety of methods, focusing on both internal evaluation and external validation. One primary approach is the Cybersecurity Program Assessment, which provides an independent maturity assessment across core critical areas. Companies like Google Cloud offer services that evaluate an organization's cybersecurity program against evolving threats and inform future strategies(Google, 2025). Similarly, firms like EY provide a Cybersecurity Program Assessment to determine if a cyber posture is adequately set up to meet these evolving threats.

Another key method is the Cybersecurity Program Controls Assessment (CPCA), which measures cyber resilience using specific categories and control questions. This type of assessment helps identify specific weaknesses in the implementation of security controls. Furthermore, tools like the Cybersecurity Assessment Tool (CAT), released by the FFIEC, are designed to help financial institutions identify their risks and determine their cybersecurity capabilities, though this is voluntary.

Regarding the question of whether there should be a regulatory requirement for external audits, there are both pros and cons. Pros of external audits include improved transparency, as an outside auditor can provide an unbiased assurance to stakeholders that the company's finances and operations are in order (Caseware, 2023). External auditors often bring a unique perspective and unbiased expertise, which can be more detailed and in-depth than internal audits (SafetyIQ, 2024). This can enhance the credibility of the organization's security posture.

However, there are also cons to consider. While not explicitly detailed in the provided snippets for mandatory external audits, potential drawbacks could include cost, the time commitment required, and the possibility of disrupting normal operations. Internal auditors, on the other hand, provide extensive knowledge and convenience, though they may lack the unbiased perspective of external auditors (Kazmierski, 2023). The decision on mandatory external audits often involves balancing the benefits of enhanced assurance and transparency against the costs and operational impacts.

References:

Caseware. “Internal vs. External Auditing.” *Caseware USA*, 27 July 2023, www.caseware.com/us/resources/blog/internal-vs-external-auditing. Accessed 22 Aug. 2025.

Google. “Cybersecurity Program Assessment.” *Google Cloud*, 2025, cloud.google.com/security/resources/datasheets/consulting-services-cyber-security-program-assessment.

Kazmierski, Nathan. “The Pros and Cons of Internal vs. External Auditing.” *Www.gtaaccounting.ca*, 22 May 2023, www.gtaaccounting.ca/blog/the-pros-and-cons-of-internal-vs-external-auditing.

SafetyIQ. “The Pros & Cons of Internal vs External Auditors - SafetyIQ.” *SafetyIQ - Predictability at Work.*, 19 Jan. 2024, safetyiq.com/insight/internal-vs-external-auditor. Accessed 22 Aug. 2025.