IS Security Policy Analysis

Case Study

Regional Bank Policy Corrections/Analysis

K. Stewart

Scenario: A *Regional Bank has been growing rapidly. In the past two years, it has acquired six smaller financial institutions. The long-term strategic plan is for the bank to keep growing and to "go public" within the next three to five years. FDIC regulators have told management that they will not approve any additional acquisitions until the bank strengthens its information security program. The regulators commented that the Regional Bank's information security policy is confusing, lacking in structure, and filled with discrepancies. Your task is to analyze and fix the policy so the regional bank can continue its growth by acquisition strategy.*

Introduction

Current Problem: The major problem here in my estimation is regulators won't allow the bank to expand its acquisitions any further without unraveling problems with the bank's information security policy. To me this is an instance of information security interfering with business operations or making operations more difficult. The solution to this problem would be to immediately fix the policy and bring it up to regulator's standards first so the bank can continue its acquisitions and reach its goal of going public.

Where to begin on this project

(Initial Step) Interview or review regulator notes: Even before I start the initial assessment, I would interview the regulators or review their notes from their findings so that as I assess the problem, I can focus in on what they need as well to keep the business growth strategy moving forward.

Step one (1) Policy Assessment: Start with a policy assessment.

Step two (2) Review old policy: For any content I can use that is "salvageable" relevant and workable in the new policy doing this will save time; this will also assist in step three doing a "gap analysis."

Step three (3) Gap Analysis: After assessing the flaws/discrepancies within the policy and combing through the current policy for any "salvageable content" do a "gap analysis" to find the holes by comparing the policy to industry-specific policies within the financial sector.

Document Request

Internal Documents: The type of documentation I would request would be any relevant internal documents like compliance reports, previous audits, and risk assessments. This is crucial in my quest to unravel all the possible issues with the bank's discrepancies found by regulators.

Regulatory Requirements: What regulations do we have to follow? I would pull up all relevant regulations and requirements for this specific industry to ensure I was on the right track in terms of fixing up any discrepancies.

Interview list

1) The author of the original policy
2) Senior management/key stakeholders
3) Key regulators who performed audit
4) IT Security personnel
5) Compliance officers
6) Risk management teams
7) Branch manager of bank to make sure we are all on the same page

The bank working towards ISO certification

Yes absolutely, but in my opinion, this is only a priority if this pleases regulators so the bank can continue its growth strategy, if this is not important to regulators then this becomes secondary.

ISO 27002:2013 domains and sections to include

- Access Controls
- Communication security
- Compliance
- Information security policies
- Information security incident management

Would you use NIST's Cybersecurity Framework (CIA security model) and related tools?

Yes, I would use the framework only if it was an immediate fix for regulators. In my interview with regulators, I would ask about using NIST CSF and if it satisfies their requirements.

The three main forms of communication to send the policy:

- e-mail for quick and inexpensive dissemination
- An intranet where employees can login and review
- Online employee digital training manuals

Mandatory Employee Compliance Training

In conclusion, another key element I will add to all of this is an intensive self-paced employee training program on compliance of which I will ask senior management to make mandatory for all employees. Adding this into the fray I think will round off keeping the bank up to speed on all compliance issues.

References

ACI Learning Launches Proprietary AI-Powered Skills Gap Analysis Tool. (2023, July 13). PR Newswire.

Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal: A Global Perspective, 30(4), 189–204. https://doiorg.libraryresources.columbiasouthern.edu/10.1080/19393555.2020.1834649

How to perform a security gap analysis article: Chris Bell (CIO 2015) https://www.cio.com/article/251153/how-to-conduct-an-information-security-gap-analysis.html

Santos, O. (2018). *Developing Cybersecurity Programs and Policies* (3rd ed.). Pearson Technology Group. **https://online.vitalsource.com/books/9780134858548**