Assignment 2: Summer 2023 – Due June 11 2023. This assignment is worth 5 marks

Please have a title page which includes:

* Your Full Name,
* Student ID,
* Course Name,
* Assignment #,
* Date,

For the Assignment please use:

* Calibri 12 Font.
* 1.5 spacing in your response.
* No more than 2 pages.
* If you are to “plagiarize” please cite your work.
* For responses which are cut, and paste will receive an immaculate “0”.

When saving the file, please use the convention of:

* Last Name Course# and Assignment # and Date.

**Failure to follow these simple rules will result in close to an immaculate “0”. 😊 No kidding!**

After Reading this article, answer the following questions – keep in mind what you have learnt thus far regarding ENRON, Frameworks, ISACA ethics, policies, procedures, standards, and Risk Management and how all this ties into to auditing. Read the following article at

<https://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO>

# Bangladesh Bank exposed to hackers by cheap switches, no firewall: police By [Serajul Quadir](https://www.reuters.com/journalists/serajul-quadir" \t "_blank)

DHAKA (Reuters) - Bangladesh’s central bank was vulnerable to hackers because it did not have a firewall and used second-hand, $10 switches to network computers connected to the SWIFT global payment network, an investigator into one of the world’s biggest cyber heists said.

The shortcomings made it easier for hackers to break into the Bangladesh Bank system earlier this year and attempt to siphon off nearly $1 billion using the bank’s SWIFT credentials, said Mohammad Shah Alam, head of the Forensic Training Institute of the Bangladesh police’s criminal investigation department.

“It could be difficult to hack if there was a firewall,” Alam said in an interview.

The lack of sophisticated switches, which can cost several hundred dollars or more, also means it is difficult for investigators to figure out what the hackers did and where they might have been based, he added.

Experts in bank security said that the findings described by Alam were disturbing.

“You are talking about an organization that has access to billions of dollars and they are not taking even the most basic security precautions,” said Jeff Wichman, a consultant with cyber firm Optiv.

Tom Kellermann, a former member of the World Bank security team, said that the security shortcomings described by Alam were “egregious,” and that he believed there were “a handful” of central banks in developing countries that were equally insecure.

Kellermann, now chief executive of investment firm Strategic Cyber Ventures LLC, said that some banks fail to adequately protect their networks because they focus security budgets on physically defending their facilities.

## POLICE BLAME BANK, SWIFT

Cyber criminals broke into Bangladesh Bank’s system and in early February tried to make fraudulent transfers totaling $951 million from its account at the Federal Reserve Bank of New York.

Most of the payments were blocked, but $81 million was routed to accounts in the Philippines and diverted to casinos there. Most of those funds remain missing.

The police believe that both the bank and SWIFT should take the blame for the oversight, Alam said in an interview.

“It was their responsibility to point it out but we haven’t found any evidence that they advised before the heist,” he said, referring to SWIFT.

A spokeswoman for Brussels-based SWIFT declined comment.

SWIFT has previously said the attack was related to an internal operational issue at Bangladesh Bank and that SWIFT’s core messaging services were not compromised.

A spokesman for Bangladesh Bank said SWIFT officials advised the bank to upgrade the switches only when their system engineers from Malaysia visited after the heist.

“There might have been a deficiency in the system in the SWIFT room,” said the spokesman, Subhankar Saha, confirming that the switch was old and needed to be upgraded.

“Two (SWIFT) engineers came and visited the bank after the heist and suggested to upgrade the system,” Saha said.

## GLOBAL WHODUNIT

The heist’s masterminds have yet to be identified.

Bangladesh police said earlier this week they had identified 20 foreigners involved in the heist but they appear to be people who received some of the payments, rather than those who initially stole the money.

Bangladesh Bank has about 5,000 computers used by officials in different departments, Alam said.

The SWIFT room is roughly 12 feet by 8 feet, a window-less office located on the eight floor of the bank’s annex building in Dhaka. There are four servers and four monitors in the room.

All transactions from the previous day are automatically printed on a printer in the room.

The SWIFT facility should have been walled off from the rest of the network. That could have been done if the bank had used the more expensive, “managed” switches, which allow engineers to create separate networks, said Alam, whose institute includes a cyber-crime division.

Moreover, considering the importance of the room, the bank should have deployed staff to monitor activity round the clock, including weekends and holidays, he said.

1. From the above article and from what you know of COBIT, NIST or other, frameworks, how important are policies and procedures to a company? Why is Policy different from procedure?
2. Do you believe the Central Bank of Bangladesh has a security framework like NIST or ISO 27001 etc. in place? Explain your answer
3. Do you believe there were unethical players at the Central Bank of Bangladesh? Explain your answer.
4. In your opinion, which Risk Treatment Plan did the Central Bank of Bangladesh apply? Explain your reasoning.
5. As a freshly minted auditor, what would be your recommendation? Provide only one and explain why?