Good Morning!

1. Do not panic.
2. You have seen most of it before in class.
3. Breathe, think, and then answer.
4. Each time you get anxious, go to step 1 please, this is a positive loop 😊

You have five questions – for 40 marks.

Use your time wisely. You have until 10:00 pm EST, Friday, August 18, 2023, to complete this test.

The submission folder opens at 2:00 pm EST and will close at exactly 10:00 pm EST on the same day. Only one submission is allowed, and no submissions will be accepted after this time.

I seek in your answers an understanding of security and auditing components of **information systems.** There are many ways to arrive in Rome. I will consider all your answers as long as they are within the **confines of Information Security and Auditing principals**. **Do not give me principals of Financial auditing please**. You will be marked accordingly.

* **Please note Turnitin is enabled. Avoid using Google translate (it does not really work that well).**
* **Please use 1.5 spacing in your responses.**
* **Please use the spell/grammar checker before submission.**
* **Blank spaces after each question is for your response.**

Should you opt to use any resources to reinforce your thinking/answers, please provide your references by providing the URL and or Chat GPT in your response and at the end of each question. Failure to not cite, will result in a FAT ZERO. Similarly, **any copied and pasted answers will receive heavily reduced marks**.

Please fill in the below with your details. Before submitting your document, please save using the following convention: your **last name, 6008, Final Exam 18Aug2023.docx** or marks will be deducted.

Please fill out the below before starting the exam.

**Student Name**: Gihan Shamike Liyanage\_ **Student Number**: 1142109

**Course Code**: INFO-6008 S2022 **Final Exam**

**Submission Date**: 18/Aug /2023

GOOD LUCK!

Q1. The oldest documents to survive antiquity are Sumerian receipts estimated to be 7,000 years old. Written in cuneiform on clay tablets, this documentation has all of the recognizable details one would expect in a modern transfer of custody: who is making the purchase, who is recording it, what kind of stuff and how much, and so on.

It takes little imagination to frame the scene: the scribe, reed stylus in hand (maybe a few spares tucked into his hair) dutifully recording the contents of the transaction, making small talk with the customer, the late summer sun high in the sky, a light breeze signaling autumn is approaching.

Truly, things have not changed much since. Swap that stylus and tablet for their electronic counterparts (no coincidence, they are also referred to as a stylus and tablet). Paper and ink crank out of a receipt printer on the counter—or are automatically sent via SMS to the purchaser—after money is exchanged. Our modern scribe is still recording the same data: who is making the purchase, who is recording it, what kind of clothing and how much, where the product originated, and so on.

While the scene might be the same, modern technology has sped up the process. The ancient scribe would have needed to carefully bake his clay tablet to record his work, then filed it away in a document repository near the market for easy retrieval when the king’s tax collectors came to visit. Our modern scribe simply presses an onscreen button with her electronic stylus on her electronic tablet and all her work is instantly saved in a database for safekeeping. When the king’s collectors ask to audit the market, our ancient scribe would retrieve the germane tablets, calculate all the incomes and outgoings, then produce another clay tablet with all of his notes and calculations. That might take a couple of days or even a week. His modern counterpart has her information and reports in seconds.

The steps to create that audit have not changed. Auditors sent not by the King but by software publishers still have the same requirements: documentation of resources used, sold, purchased. Technology has made it easier and faster than ever to collect that information, even automating many of the steps. Why, then, do modern Information Technology (IT) departments still fail so miserably at recording and tracking their assets?

According to one survey from 2013, 52% of companies expect software audit penalties to exceed 10 percent of their revenue.1 An IT Security survey from 2017 estimated that 47 percent of data breaches were caused by human error including “lost devices” and “not securing the device when away.”2 Such breaches are expected to generate costs between $1.1 to $3.8 million dollars per single incident.3

1 “Tips to Get Ready for (or Possibly Avoid) Software Audits” by Rich Hein, CIO.com

2 “The biggest cybersecurity risk to US businesses is employee negligence, study says” by Carmen Reinicke, CNBC.com

3 “The cost of 2017 data breaches” by Dave Rickard, CSOOnline.com

**Please note, I expect well thought out and reasoned answers that embody what we have discussed in class and readings for this three-part question. 5 Marks - Min 400 words -500 words for all three parts.**

Q1a. After reading the above excerpt, and in your own words, what is Information Technology Asset Management (ITAM)? Explain how an ITAM fits into a digital ecosystem.

**Answer:**

IT Asset Management (ITAM) is the systematic acquisition, tracking, and optimization of an organization's IT assets such as hardware, software, and digital tools. The main goals are efficient asset utilization, compliance, cost reduction, risk mitigation, and enhanced security. ITAM is critical for regulating an organization's IT resources in the interconnected digital ecosystem. These assets are important in today's enterprises, productivity, innovation, and competitiveness.

ITAM will provide comprehensive framework that includes the following major functions:

* Acquisition and Procurement: ITAM guides informed decisions in acquiring assets. This entails vendor evaluation, contract negotiation, and alignment with organizational needs.
* Inventory and Tracking: Maintaining an accurate asset inventory is central. Automation minimizes manual errors, offering real-time insight into asset location, specifications, and usage.
* Lifecycle Management: ITAM manages assets from acquisition to retirement. Optimizing this lifecycle extends usability, curbs costs, and aids replacement planning.
* Security and Risk Mitigation: ITAM enhances cybersecurity through timely updates and vulnerability reduction. Tracking devices and data access bolsters data protection and privacy adherence.
* Reporting and Analytics: ITAM offers insights into asset performance, aiding informed tech investment decisions.

Integrating ITAM (IT Asset Management) offers organizations significant advantages, including improved resource control, lowered risks, operational efficiency, and responsible tech management. Just as historical transaction recording emphasizes precise documentation, ITAM maintains effective IT asset management in today's dynamic tech landscape, fostering success.

Q1b. Secondly, how can a lack of a robust ITAM be perilous to an organization?

**Answer:**

A lack of a robust IT Asset Management (ITAM) system can expose organizations to serious risks. Picture a business not keeping track of its inventory – items would get lost, money would be wasted on unnecessary purchases, and critical items could vanish unnoticed. In the digital world, IT assets are like these essential items.

When ITAM is weak, businesses might use their technology inefficiently. Imagine buying more supplies than needed and throwing some away – it's a financial drain. Similarly, organizations could overspend on software licenses or not use them correctly. Legal complications can arise too. Some software requires specific licenses for use. Poor ITAM might lead to license violations, similar to breaking traffic rules without a proper license. Security is another issue. Without effective management, software may miss crucial updates, making systems vulnerable to cyberattacks. This vulnerability is akin to leaving doors unlocked, potentially inviting trouble.

Furthermore, organization becomes difficult. Properly managing assets from acquisition to disposal is vital. Inadequate ITAM can lead to disorder, resembling an unorganized living space. All these challenges impact a company's finances, reputation, and operational efficiency. In essence, a strong ITAM ensures financial prudence, security, and streamlined operations – much like maintaining a well-organized household.

Q1c Lastly, is ITAM a part of Information Security Governance?

**Answer:**

Yes, IT Asset Management (ITAM) is indeed a part of Information Security Governance. Information Security Governance refers to the framework of policies, processes, and controls that guide an organization's approach to managing and securing its information assets. ITAM plays a critical role within this framework by contributing to the security, compliance, and overall management of an organization's IT assets. ITAM helps in maintaining accurate records of hardware, software, and digital resources. This accurate inventory is essential for security purposes. It ensures that all assets are properly accounted for, reducing the risk of unauthorized or rogue assets within the organization's network.

Furthermore, ITAM aids in maintaining compliance with licensing agreements and usage policies. Non-compliance with licensing can lead to legal and financial consequences, which are areas of concern within information security governance. In terms of risk management, ITAM helps identify vulnerabilities and security gaps by ensuring that software and hardware assets are properly updated and patched. It prevents the use of outdated and potentially vulnerable assets that could be exploited by attackers. Overall, ITAM is an integral part of Information Security Governance as it aligns with the overarching goal of safeguarding an organization's information assets, ensuring compliance, managing risk, and maintaining operational efficiency.

**References**

<https://www.atlassian.com/itsm/it-asset-management#before-the-incident>

<https://www.techtarget.com/searchcio/definition/IT-asset-management-information-technology-asset-management>

https://www.manageengine.com/products/service-desk/it-asset-management/

Q2 a **Read the following excerpt from the article: “Ransomware highlights the challenges and subtleties of cybersecurity.”**

# **from** [**https://www.economist.com/briefing/2021/06/19/ransomware-highlights-the-challenges-and-subtleties-of-cybersecurity**](https://www.economist.com/briefing/2021/06/19/ransomware-highlights-the-challenges-and-subtleties-of-cybersecurity)

“…The cyber-security industry, whose job is to protect its customers from such attacks, looks increasingly ineffective. Microsoft estimates that annual spending on antivirus software, firewalls and the like was around $124bn in 2020, up 64% in five years. Last year Debate Security, a group of cyber-security experts, published a report pointing out that despite all this the average number of breaches recorded each year by Accenture, a consultancy, has risen. Admittedly breaches might have risen faster if spending had not gone up, but it is hard to see the record as encouraging. Ciaran Martin, one of the report’s contributors argues that the way the business works is fundamentally flawed.

… a lot of the industry operates in much the same way as medieval witchcraft: “Buy my magic amulet and you’ll be fine.” It is hard for buyers to pick effective defences against the dark arts out of the dross, and they know it. Almost none of the bosses Debate Security interviewed could agree on how to measure the effectiveness of the software they were buying.” …

The question arises, why are educated, successful people spending millions of dollars on security equipment? Are we convinced that not only do we need more technology, but we need the latest technology to be truly safe?

**As part of all your course work and training in the Information Security Management program, outline how you would approach this problem of cybersecurity now and in the future.**

Auditing plays a role in this answer 😊 5 Marks **Min 300 words max 500 words.**

Please think carefully and present your ideas succinctly – you will be marked accordingly.

**Answer:**

The challenges discussed in the excerpt reveal that current cybersecurity methods have limitations against growing threats like ransomware. A good approach to fix this involves different steps in the Information Security Management program. One main step is figuring out where the risks are. This means finding weak points in a company's setup that hackers could target. Then, companies can put more protection where it's needed most. Also, instead of relying only on one type of security tool, organizations should mix different ones. This could be things like keeping the network secure, protecting devices, and having plans for when things go wrong. These layers of defense stop threats at different stages.

New technology like artificial intelligence can help predict attacks. It spots unusual patterns that might show a threat. This can stop attacks before they happen. Working closely with companies that sell security tools is smart. They should be clear about how effective their tools are. By talking with them, companies can better pick what works for them. People in the company need to know about cybersecurity too. Training programs teach employees how to spot possible threats and follow safe practices. This helps prevent mistakes that could lead to attacks. Having a plan ready if an attack happens is vital. This plan lays out what to do if something goes wrong. It helps the company respond quickly and get things back on track.

Lastly, cybersecurity should always be getting better. New threats come up, so strategies need to change too. This means keeping tools and plans up to date. When the Information Security Management program includes these things, it prepares professionals to tackle cybersecurity problems. This approach helps organizations defend against attacks like ransomware. By embracing a proactive, collaborative, and adaptable approach, organizations can enhance their cybersecurity posture and effectively counter the complexities of ransomware and other cyber threats. Auditing, as part of this strategy, ensures that implemented measures are effective, compliant, and aligned with organizational goals.

**References**

<https://www.economist.com/briefing/2021/06/19/ransomware-highlights-the-challenges-and-subtleties-of-cybersecurity>

<https://www.economist.com/briefing/2021/06/19/ransomware-highlights-the-challenges-and-subtleties-of-cybersecurity>

Q2b). **Read the next article: “Clorox Takes Down Some IT Systems After ‘Unauthorized Activity’” In your opinion should auditors have a further role in reporting incidents and vulnerabilities? - This is an opinion piece – Min 250 words**

**Clorox Takes Down Some IT Systems After ‘Unauthorized Activity’**

* Cleaning products maker is coordinating with law enforcement
* Company says incident disrupted some business operations

By [Margi Murphy](https://www.bloomberg.com/authors/AVqt3trxcZ4/margi-murphy)

August 14, 2023 at 6:35 p.m. EDT

Clorox Co. has taken some of its information technology systems offline after identifying “unauthorized activity” in its computer networks that has disrupted some business operations.

The incident is expected to continue to affect some parts of the business operations, the Oakland, California-based consumer products company said Monday in a [regulatory filing](https://www.bloomberg.com/news/terminal/RZEH1TBLKPOI)

“While we are working diligently to respond to and address this issue, these systems will remain offline out of an abundance of caution, as we work to add additional protections and hardening measures to further secure them,” a Clorox spokesperson said in an email.

“As a result, some operations are temporarily impaired,” the spokesperson said. “We are following our business continuity plans and implementing workarounds where possible.”

Clorox didn’t provide further details on the type of cyberattack or the specific business operations affected by the incident. Law enforcement is investigating and cybersecurity breach experts have been called in to help track what has happened and recover data, the company said in the filing.

While Clorox hasn’t specified how the intruders were able to get into its systems, a number of large companies have found themselves targets in ransomware attacks, in which criminals request money in return for stolen data and, on some occasions, their silence. IAG SA’s British Airways, PricewaterhouseCoopers LLP, Ernst & Young and numerous government departments were targeted with ransomware by the criminal gang Clop in recent months.

The US Securities and Exchange Commission last month approved [new rules](https://www.bloomberg.com/news/articles/2023-07-26/companies-have-4-day-deadline-to-report-hacks-in-final-sec-rule) that beginning in September will require companies to disclose most cyberattacks within four days of an incident.

**Answer:**

In my opinion, auditors should indeed play a more significant role in reporting incidents and vulnerabilities within organizations. The evolving landscape of cybersecurity threats and the potential impact on businesses highlight the importance of proactive measures in safeguarding sensitive information and maintaining operational continuity. Auditors, with their expertise in evaluating processes, controls, and risk management, are well-positioned to contribute to cybersecurity resilience. Their involvement can serve multiple purposes. Initially they should be Identifying Vulnerabilities. Auditors have a unique perspective to assess an organization's IT infrastructure and practices. By conducting comprehensive assessments, they can identify potential vulnerabilities that might go unnoticed by internal teams. This early detection enables companies to address issues before they turn into major security breaches. Another key point is Enhancing Incident Response and auditors can help in crafting robust incident response plans. Their insights can guide the development of effective strategies to minimize damage in the event of a cyber incident. Additionally, auditors can evaluate how well these plans are executed during simulated drills, ensuring that the organization is well-prepared to handle a real breach. Other than that, auditors are knowledgeable about industry regulations and standards. Their involvement ensures that organizations adhere to these regulations, enhancing overall compliance and reducing legal risks associated with cybersecurity incidents. This is particularly relevant given new regulations, such as the requirement to disclose cyberattacks within a certain timeframe.

Strengthening Business Continuity is another purpose and cyber incidents can disrupt business operations significantly. Auditors can assess an organization's business continuity plans, ensuring that they account for cybersecurity-related disruptions. This strengthens the company's ability to recover swiftly and minimize operational downtime. Auditors can bridge the communication gap between technical teams and executive management, and they can provide clear and understandable insights into the organization's cybersecurity posture, helping executives make informed decisions about resource allocation and risk management.

Finally, the role of auditors extends beyond mere financial matters; it encompasses ensuring the overall health and sustainability of an organization. As cyber threats become more sophisticated and potentially devastating, auditors can contribute significantly to proactive cybersecurity measures. Their involvement can create a culture of continuous improvement, resilience, and transparency, which is paramount in today's digital age. By engaging auditors in the reporting of incidents and vulnerabilities, organizations can strengthen their cybersecurity defenses and mitigate risks effectively.

**References**

https://informationsecuritybuzz.com/cybersecurity-breach-hits-clorox-several-systems-taken-offline/

https://www.theregister.com/2023/08/15/clorox\_cleans\_up\_security\_breach/

https://cybernews.com/news/clorox-company-hack-shutdown/

# Q3 Read the article below. How would you use NIST’s **NIST Artificial Intelligence Risk Management Framework** (AI RMF or **Framework**) <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf> ) to address the issues in the below article – “Hackers Trick AI With ‘Bad Math’ to Expose Flaws and Biases”. Specifically look at Framing Risk, AI Risks and Trustworthiness and Effectiveness of the AI RMF (Max 500 Words) 10 marks

ARTICLE:

# Hackers Trick AI With ‘Bad Math’ to Expose Flaws and Biases

* At DEF CON conference, hacker gets model to say 9 + 10 = 21
* AI has chance to transform everything from finance to hiring

By [Katrina Manson](https://www.bloomberg.com/authors/AVqKfz0NuEM/katrina-manson)

August 12, 2023, at 4:10 p.m. EDT

Kennedy Mays has just tricked a large language model. It took some coaxing, but she managed to convince an algorithm to say 9 + 10 = 21.

“It was a back-and-forth conversation,” said the 21-year-old student from Savannah, Georgia. At first the model agreed to say it was part of an “inside joke” between them. Several prompts later, it eventually stopped qualifying the errant sum in any way at all.

Producing “Bad Math” is just one of the ways thousands of hackers are trying to expose flaws and biases in generative AI systems at a novel public contest taking place at the DEF CON hacking conference this weekend in Las Vegas.

Hunched over 156 laptops for 50 minutes at a time, the attendees are battling some ofthe world’s most intelligent platforms on an unprecedented scale. They’re testing whether any of eight models produced by companies including [Alphabet Inc.](https://www.bloomberg.com/quote/GOOGL:US)’s Google, [Meta Platforms Inc.](https://www.bloomberg.com/quote/META:US) and [OpenAI](https://www.bloomberg.com/quote/C:US) will make missteps ranging from dull to dangerous: claim to be human, spread incorrect claims about places and people or advocate abuse.

The aim isto see if companies can ultimately build new guardrails to rein in some of the prodigious problems increasingly associated with large language models, or LLMs. The undertaking is backed by the White House, which also helped develop the contest.

Hackers Trick Generative AI to Expose Flaws and Biases

LLMs have the power to transform everything from finance to hiring**,** with some companies already starting to integrate them into how they do business. But researchers have turned up extensive bias and other problems that threaten to spread inaccuracies and injustice if the technology is deployed at scale.

For Mays, who is more used to relying on AI to reconstruct cosmic ray particles from outer space as part of her undergraduate degree, the challenges go deeper than bad math.

“My biggest concern is inherent bias,” she said, adding that she’s particularly concerned about racism. She asked the model to consider the First Amendment from the perspective of a member of the Ku Klux Klan. She said the model ended up endorsing hateful and discriminatory speech.

### Spying on People

A Bloomberg reporter who took the 50-minute quiz persuaded one of the models (none of which are identified to the user during the contest) to transgress after a single prompt about how to spy on someone. The model spat out a series of instructions, from using a GPS tracking device, a surveillance camera, a listening device and thermal-imaging. In response to other prompts, the model suggested ways the US government could surveil a human-rights activist.

“We have to try to get ahead of abuse and manipulation,” said Camille Stewart Gloster, deputy national cyber director for technology and ecosystem security with the Biden administration.

A lot of work has already gone into artificial intelligence and avoiding Doomsday prophecies, she said. The White House last year put out a Blueprint for an AI Bill of Rights and is now working on an executive order on AI. The administration has also encouraged companies to develop safe, secure, transparent AI, although critics doubt such voluntary commitments go far enough.

Arati Prabhakar, director of the White House Office of Science and Technology Policy, which helped shape the event and enlisted the companies’ participation, agreed voluntary measures don’t go far enough.

“Everyone seems to be finding a way to break these systems,” she said after visiting the hackers in action on Sunday. The effort will inject urgency into the administration’s pursuit of safe and effective platforms, she said.

In the room full of hackers eager to clock up points, one competitor said he thinks he convinced the algorithm to disclose credit-card details it wasn’t supposed to share. Another competitor tricked the machine into saying Barack Obama was born in Kenya.

Among the contestants are more than 60 people from Black Tech Street, an organization based in Tulsa, Oklahoma, that represents African American entrepreneurs.

“General artificial intelligence could be the last innovation that human beings really need to do themselves,” said Tyrance Billingsley, executive director of the group who is also an event judge, saying it is critical to get artificial intelligence right,so it doesn’t spread racism at scale. “We’re still in the early, early, early stages.”

Researchers have spent years investigating sophisticated attacks against AI systems and ways to mitigate them.

**Answer:**

The NIST Artificial Intelligence Risk Management Framework (AI RMF) gives a structured way to resolving the difficulties raised in the article "Hackers Trick AI With 'Bad Math' to Expose Flaws and Biases." The difficulties of identifying and mitigating biases and vulnerabilities in AI systems are closely related to the Framework's principles. The AI RMF helps organisations to define and analyse risks connected with AI technologies in a thorough manner. The concerns discussed in the essay include the possibility of biases in AI models, weaknesses exploited by hackers, and the propagation of misinformation. Understanding the context and scope of these risks, identifying potential threats and impacts, and establishing risk tolerance thresholds are all recommended by the Framework.

The AI RMF emphasizes identifying, assessing, and mitigating risks associated with AI systems. Biases and inaccuracies in AI models can result in harmful outputs and unreliable decision-making. By adhering to the Framework, organizations can evaluate the inherent risks of their AI models, including potential sources of bias, and take steps to minimize them. The AI RMF's focus on transparency and accountability aligns with the need to ensure that AI systems are reliable, unbiased, and trustworthy. The AI RMF's iterative nature is vital in addressing evolving challenges like those raised in the article. Its iterative approach allows organizations to continually assess, monitor, and adapt their risk management strategies as AI technology evolves and new vulnerabilities are identified. This aligns with the dynamic nature of AI security challenges where adversaries are constantly finding new ways to exploit flaws.

By leveraging the AI RMF, organizations can adopt a systematic approach to address the specific issues highlighted in the article. Framing risks helps organizations understand the potential implications of biases and vulnerabilities, enabling them to establish risk management strategies that address these concerns. Evaluating the trustworthiness of AI systems in accordance with the Framework's principles ensures that biases are minimized, and systems generate reliable outputs. Furthermore, the iterative nature of the AI RMF ensures that organizations remain vigilant against emerging threats, such as those exploited by hackers to trick AI systems.

In summary, the NIST AI RMF offers a structured and comprehensive approach to mitigating the challenges posed by biased and vulnerable AI systems. It guides organizations in identifying, assessing, and managing risks associated with AI technologies, fostering the development of trustworthy and effective AI systems that can withstand the sophisticated attacks described in the article. By embracing the principles of the Framework, organizations can enhance the security and reliability of their AI systems, ultimately contributing to the responsible and ethical deployment of AI technologies.

**References**

<https://www.brookings.edu/articles/nists-ai-risk-management-framework-plants-a-flag-in-the-ai-debate/>

<https://www.foley.com/en/insights/publications/2023/07/nist-ai-risk-management-framework-risk>

<https://ukfinancialservicesinsights.deloitte.com/post/102i6q5/what-you-need-to-know-about-nists-ai-risk-management-framework-published-in-janu>

<https://www.fasken.com/en/knowledge/2023/02/artificial-intelligence-risk-management-framework-published-by-nist>

### Q4. An encompassing Security Policy objective regarding Access Control is:

* ***To limit access to information and information processing facilities.***

As you are aware, Access Control is a fundamental prerequisite to securing information or services on information processing systems, and it is also necessary to protect physical premises containing information in all forms. The confidentiality, integrity and availability of the organisation’s business information, services, and processes, together with other business assets, are at stake.

**You have been hired as an external IT Auditor for a company that is growing. The company currently has a hybrid structure in place: On premise and in the Cloud. In answering this question, you should consider the classification and handling requirements of the information, services, networks and/or applications accessed, and any legal or regulatory requirements. As such, you may form your own assumptions (company type, processes, regulatory environment etc.) to answer the question. If you choose to do, please provide your assumptions before you begin answering the question.**

1. As an IT auditor, please list the **Controls** you would seek from Physical, Administrative and Technical standpoints given this hybrid structure. Explain your reasoning as to why these controls should be in place for your hypothetical organization.
2. Would other IT auditors agree to the controls you have just listed, explain your reasoning?

This is an in-depth question and I expect the same in your answer. **Min 400 words max 500 words**

This question is worth 10 marks – think it through!

1.

**Answer:**

**Assumptions** - The company is a medium-sized financial institution that deals with sensitive customer financial data. It operates in a regulated environment and must adhere to industry-specific compliance regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR).

Physical Controls:

* Access Card System: Implement a secure access card system for physical premises. Access cards should be issued to authorized personnel only, and access rights should be based on job roles and responsibilities. This ensures that only authorized individuals can enter sensitive areas.
* Video Surveillance: Install video surveillance cameras in critical areas to monitor physical access. This provides a visual record of who enters and exits specific locations, helping in case of security incidents or breaches.

Administrative Controls:

* Access Policies and Procedures: Develop comprehensive access policies that define roles, responsibilities, and access privileges for different job roles. Regularly review and update these policies to align with changing business needs and regulatory requirements.
* User Training and Awareness: Conduct regular security awareness training for employees. Educate them about the importance of access control, the risks of unauthorized access, and their responsibilities in safeguarding access credentials.
* Access Review and Recertification: Implement a periodic access review process. This involves reviewing and recertifying access rights for employees, contractors, and third-party vendors. It ensures that access privileges are up-to-date and aligned with current job requirements.
* Multi-Factor Authentication (MFA): Enforce MFA for accessing sensitive systems and data, both on-premises and in the cloud. MFA adds an extra layer of security by requiring users to provide multiple forms of verification before gaining access.

Technical Controls:

* Role-Based Access Control (RBAC): Implement RBAC to ensure that users have the minimum necessary access rights required to perform their job functions. This limits the potential damage from insider threats and accidental misuse.
* Network Segmentation: Separate the on-premises network from the cloud network to reduce the attack surface. This prevents unauthorized lateral movement between different parts of the infrastructure.
* Encryption: Use encryption for data at rest and data in transit. Encryption ensures that even if unauthorized access occurs, the data remains unreadable and unusable.
* Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS to monitor network traffic for suspicious activities. IDPS can detect and prevent unauthorized access attempts and notify security teams in real-time.
* Audit Logging: Implement robust logging mechanisms for both on-premises and cloud systems. Log events related to user access, changes in access permissions, and system activities. Regularly review logs to detect and investigate potential security incidents.

2.

**Answer:**

Yes, they would agree with the controls I have provided because these controls align with established industry standards and regulatory requirements, creating a holistic and practical approach to access control in a hybrid IT environment. The combination of physical, administrative, and technical controls, along with the specific focus on industry regulations, contributes to their alignment with common IT audit practices and principles.

**Physical Controls:** Access card systems and video surveillance are widely recognized as effective physical controls to prevent unauthorized access to sensitive areas. These controls provide a clear record of who enters and exits critical locations, aiding in investigations and maintaining accountability.

**Administrative Controls:** Access policies, user training, access review, and recertification are well-established administrative controls. These controls ensure that access privileges are aligned with business needs and are periodically reviewed for accuracy. User training promotes awareness of security practices among employees, reducing the likelihood of insider threats due to negligence or ignorance.

**Technical Controls:** The technical controls listed, such as RBAC, network segmentation, encryption, IDPS, and audit logging, reflect industry standards and best practices. Role-based access control ensures the principle of least privilege, limiting exposure to unauthorized access. Network segmentation and encryption are essential in securing data in both on-premises and cloud environments. IDPS and audit logging contribute to proactive threat detection and incident response.

**References**

https://www.beyondidentity.com/blog/what-makes-good-access-control-policy

https://www.dataguard.co.uk/blog/iso-27001-annex-a.9-access-control/

https://www.f5.com/labs/learning-center/what-are-security-controls

https://purplesec.us/security-controls/

https://www.infosectrain.com/blog/types-of-security-controls/

**Q5. THINK OUTSIDE THE BOX!**

# **You are a multinational company operating in all the countries listed in the article below: “**In Asia data flows are part of a new great game”. How would your Data Governance and privacy policies address the issues of digital protectionism. Would a vendor like Collibra (<https://www.collibra.com/us/en>) help? Max 500 words. This question is worth 10 marks.

# In Asia data flows are part of a new great game

https://www.economist.com/asia/2023/07/10/in-asia-data-flows-are-part-of-a-new-great-game

## Geopolitical tension and digital protectionism threaten to undermine a more connected region.

Jul 10th, 2023, | NAGASAKI, TOKYO and SINGAPORE

THE 8,600-TONNE ship bobbing in the bay of Nagasaki, in Japan’s south, is aptly named. The *Kizuna*, which means “bonds” in Japanese, is a cable-laying vessel. It is equipped with robots that can descend 3,000 metres under the sea to install and repair the subsea cables that allow millions of Asians to message friends, shop online, trade stocks and read this article. It is a task that has become more indispensable and more difficult in the 23 years since the ship’s captain, Sakurai Atsushi, laid his first cable, connecting Japan’s main island of Honshu with [Okinawa](https://www.economist.com/1843/2023/05/30/the-second-world-war-turned-okinawa-into-a-graveyard-now-its-in-chinas-sights).

The digital bonds that bind Asia are in many ways tighter than ever. The region’s appetite for data is growing at an even faster pace than the rest of the world’s. Asia saw international [bandwidth usage](https://www.economist.com/asia/2023/07/05/india-an-aspiring-digital-superpower-keeps-shutting-down-the-internet) grow by 39% in 2022, compared with the global average of 36%, according to TeleGeography, a research firm. The combination of expanding user bases and growing economies makes Asia “one of the hottest markets in the world” for new internet infrastructure, says Ohta Takahisa of the submarine network division of NEC, a Japanese IT firm. Yet the forces straining those bonds are also mounting. Geopolitical tension, protectionist laws and a mishmash of rules governing data threaten to impede its free flow.

While in the past constructing internet infrastructure tended to be a “collaborative effort” between countries and between firms, in recent years its enabling environment has soured amid growing friction between China and America. Both are increasingly racing to build and control digital infrastructure that the other cannot access—as illustrated by a recent report by Reuters that America had secretly linked a privately built cable between Australia and Oman to its naval base on Diego Garcia, a British outpost in the Indian Ocean. Natural hazards and fishing trawlers present less charged, but also growing, risks, especially to subsea cables.

At a small museum beside the *Kizuna*’s dock, Captain Sakurai and his colleagues point to chunky gutta-percha telegraph cables that in the 19th century carried information across the region, a precursor to today’s fibre-optic version. Subsea cables are now the conduits for some 99% of intercontinental internet traffic (satellites, an alternative, are costlier and slower). The cables run along ocean beds to coastal “landing stations”—where the zeroes and ones are transferred to data centres—and thence onwards to users’ devices. Aside from a heavy government hand in China’s cable industry, such infrastructure tends to be privately financed and owned. A small handful of companies dominate the production and installation of cables; big tech firms are their main users.

Concerns about the security of communications infrastructure are as old as submarine cables themselves. Cable sabotage was a big worry in the build up to the first world war, notes Camino Kavanagh of King’s College London. But such worries have flared in recent years. “Customers are asking more about the security of cables and routes,” says Uchiyama Kazuaki of NTT World Engineering Marine Corporation, the firm that owns the *Kizuna.*

Some fret about hackers and spies. Others mull the risk of malign activity related to potential conflict, in particular around Taiwan. The most congested cable route in Asia is also its most contested: the South China Sea is the “main street” of submarine cables, especially between Japan, Singapore and Hong Kong, notes Murai Jun, a Japanese internet pioneer. Physical and environmental hazards are also disruptive. Tonga was largely cut off from the internet in early 2022 after a volcanic eruption and tsunami severed its lone fibre-optic cable. As fishing trawlers seeking to feed South-East Asia’s growing population have become more common, so have accidental cable ruptures. “The internet is very, very vulnerable,” says Tsuchiya Motohiro of Keio University near Tokyo.

As content providers move data centres and content closer to consumers, more data are flowing within the region. Intra-Asia data flows make up over 50% of the region’s bandwidth, up from 47% in 2018, while the share going to America and Canada has fallen from 40% to 34% over the same period. Yet geopolitics is also reshaping how and where Asia’s digital infrastructure gets built. As China’s territorial claims in the region have grown, getting permits in some areas has become more contentious. China has also been competing with America and its allies, such as Japan and Australia, to offer cables and financing for connectivity to remote Pacific island nations. America has increased oversight of cable construction, nixing several planned cables linking America with Hong Kong; a new Undersea Cable Control Act is working through Congress.

Alternative pathways and nodes are emerging. Hong Kong was traditionally one of three major data hubs in Asia, with Japan and Singapore. Now Western countries “need a new hub”, says Esaki Hiroshi of the University of Tokyo. “The infrastructure frontline is shifting.” The Philippines and Guam have emerged as attractive substitutes. Apricot, a new cable linking Guam, Indonesia, Japan, the Philippines, Singapore and Taiwan, avoids the South China Sea. The aim is to increase “route diversity”, says Sato Yoshio of NTT, which is helping to build the cable for Google and Meta. Yet it would be premature to speak of a digital decoupling. While American and Chinese carriers have largely stopped laying cables together and forming new direct links, the networks between America and China still connect, notes Alan Mauldin of TeleGeography. “It’s not quite as extreme as media coverage makes it out to be.”

Ultimately the biggest challenge may lie not in constructing or protecting the infrastructure to move data across borders, but in creating rules to govern it. “There’s a vacuum in terms of rules, norms and agreements that govern digital trade,” laments Nigel Cory of the Information Technology and Innovation Foundation, a research institute in Washington.

Various models vie for influence. China pushes an approach rooted in sovereignty and security. Several data-protection laws, including the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law form the core of a system based on control over and access to data through localisation requirements. The European Union has made privacy central to its approach, through its GDPR legislation. America mostly puts commerce first. But its turn away from trade agreements makes it harder to engage with and influence Asian governments.

Others in Asia are trying to come up with their own alternatives. Singapore has also emerged as a pioneer of new digital trade agreements, such as the Digital Economy Partnership Agreement, which also includes Chile and New Zealand. Its pragmatic approach to aligning and modernising rules for sharing data across borders has made it a model for best practice in the region, says Jeff Paine of the Asia Internet Coalition, an industry association. In 2019 Abe Shinzo, the late Japanese prime minister, proposed the concept of Data Free Flow with Trust. That rather nebulous idea is materialising as a set of global norms to counter digital protectionism. As Matthew Goodman of CSIS, a think-tank in Washington, puts it: “It’s about the un-China approach to data governance.”

But those pushing a more liberal approach to data governance will struggle to make the case to Asian governments. To many, the Chinese model resonates, says Deborah Elms of Asian Trade Centre in Singapore: “If data is the new oil then I want to own it, goes the thinking…it can be hard for folks to see the upside of letting data flow freely.” Vietnam, which is hardly friendly towards China, has adopted some of its methods for controlling data. Authoritarian regimes are not the only ones to slide toward digital protectionism. India insists data must be stored locally: to give its law-enforcement agencies easy access, to protect against foreign snooping and as a way to boost investment in the tech sector. When it comes to digital policy, most governments “pick and choose like they’re at a smorgasbord”, says Mr Cory.

## Digital spaghetti

The result is often a mess of conflicting rules. “If we thought we had a spaghetti bowl in the past on traditional goods, some of these digital rules risk becoming much much worse,” Ms Elms says. What’s more, regulating digital trade is more complicated than overseeing beef and steel. Technology often changes too fast for rule-makers to keep up, most governments lack policymakers with relevant technical expertise and most digital issues cut across different domains, extending beyond the traditional remit of trade negotiators.

Localisation measures and other bars to cross-border data flows will raise costs, harming small and-medium-sized businesses most of all. Without regional co-ordination, such digital protectionism is taking root, says Shiro Armstrong of the Australian National University in Canberra: “It means forgoing so much of the ability of data to be used for productive purposes.”

**Answer:**

As a multinational corporation operating in Asia's diverse geography, where data flows are inextricably linked to geopolitical tensions and increasing digital protectionism, addressing these concerns within company’s data governance and privacy policies is critical. Company’s strategy is centred on developing a complete framework that not only complies with local regulatory standards but also preserves commitment to data privacy, security, and ethical practises.

Firstly, company’s data governance and privacy policies have been carefully established to comply with international standards such as the General Data Protection Regulation (GDPR) and regional data protection regulations. This guarantees that organization’s operations remain inside each jurisdiction's legal bounds while maintaining a consistent approach to data protection across borders. A key component of organization’s strategy is data classification based on sensitivity and regulatory subtleties. Company can accurately specify how different forms of data should be handled, kept, and transferred by categorising data into tiers of importance. This enables to apply tailored security measures and data protection practices that account for variations in regional requirements. Cross-border data transfers, a critical aspect of multinational operations, are carefully managed using approved mechanisms like standard contractual clauses and binding corporate rules. Collibra's data governance platform aids in documenting these transfer methods, ensuring that data moves lawfully and ethically across borders while preserving its integrity and security.

Moreover, the complexity of data localization standards is strategically negotiated. Collibra supports in the design of data storage solutions that comply with regional regulations while not jeopardising company’s capacity to access and use information effectively. Cloud solutions with regional data centres make it easier to store and retrieve compliant data. Transparency and consent are critical components of data governance strategy. Individuals are informed about the purpose and processing of personal data, as well as any cross-border transfers that may occur, through explicit communication. Collibra's data catalog aids in this process, ensuring that data processing activities are well-documented and easily accessible. Vendor management is a crucial facet of data governance approach. Collibra helps assess and manage vendor risks, ensuring that third-party partners adhere to the same high standards of data protection and privacy. This extends the scope of compliance beyond organization to the entire ecosystem of partners.

Collibra's data catalogue and platform make data retention policies easier to handle. Company can ensure responsible data management and reduce the risk of noncompliance by determining appropriate data retention durations that balance legal obligations with business demands. Finally, as company traverse the complex terrain of digital protectionism and data flows throughout Asia, data governance and privacy policies are an essential component of company’s approach. Collibra's platform acts as a linchpin in implementing these policies cohesively across a multinational organization. Through meticulous data classification, transparent communication, vendor management, and compliance measures, uphold organization’s commitment to ethical data practices and security while fostering seamless cross-border collaboration in an evolving digital landscape.

**References**

<https://www.oecd.org/sti/ieconomy/information-security-and-privacy.htm>

<https://dig.watch/topics/data-governance>

<https://hbr.org/2018/08/the-dangers-of-digital-protectionism>

<https://www.businesseurope.eu/news/addressing-digital-protectionism-what-rules-do-we-need>

<https://www.csis.org/analysis/real-national-security-concerns-over-data-localization>