Legendary Performance!

Congratulations on successfully completing this assignment! Your grade has been recorded. Feel free to close this tab and return to the main course page.

Required passing grade: 40%

Status: **Passed**

Final Score: 25 / 25 (100%)

Question 1 Score: 5/5

Case Study: Lightning Strikes Case Study (Part A)

In August 2015, Google's data center in Belgium experienced four consecutive lightning strikes, which caused a significant power outage. The strikes affected some disks in the data center's storage systems, leading to the loss of a small amount of user data. Google's robust redundancy and backup measures mitigated the impact, but the incident highlighted vulnerabilities in data integrity during extreme natural events. The incident also raised concerns among customers about the reliability of the company's infrastructure.

Root Cause

The incident's initial point of failure was a power failure that affected the data center's storage systems. The vulnerability arose from extended or repeated battery drain, which made certain storage systems more susceptible to power failure. A carefully managed group handled this complex issue effectively by declaring the incident early and organizing a response with clear leadership.

Actions Taken

In response to the incident, power was quickly restored with the help of automatic auxiliary systems. The Incident Commander delegated the normal problems of restoring power and rebooting servers to the appropriate Operations Lead, while engineers worked on fixing the issue and reported their progress back. The organization addressed the manual intervention required to restore the systems to their normal serving state and acknowledged the need for improvements to maximize the reliability of the data center.

Evaluate Effectiveness and Timeliness

The actions taken, including coordinated decision-making and interaction among multiple teams, effectively mitigate the impact of the incident. Minimal data loss occurred, representing less than 0.000001 percent of total disk storage space. The Incident Commander assigned appropriate operations team members from both the GCE and Persistent Disk teams to the incident, focusing on promptly addressing customer needs.

Successes, Gaps, and Failures

- **Success:** Fast power restoration with the help of automatic auxiliary systems and effective coordination led by the Incident Commander.
- **Gap:** Certain storage systems were more susceptible to power failure due to extended or repeated battery drain.
- **Failure:** Manual intervention was required to restore systems to their normal serving state.

Impact on the Organization

Question 1: What operational impacts did the organization experience due to the lightning strike incident?

- ○ Extended downtime and significant data loss
- ◉ Operational disruptions and minimal data loss ✓

  Correct. The lightning strikes caused brief power outages, disrupting the organization's ser-vices, resulting in downtime and affecting users' ability to access services. Although most data was successfully committed to stable storage, some recently written data was lost due to power failures. It affected a tiny percentage of the total disk space, but it was significant for those impacted.
- ○ Complete system failure and loss of customer data
- ○ No operational disruptions were experienced

Correct. The lightning strikes caused brief power outages, disrupting the organization's ser-vices, resulting in downtime and affecting users' ability to access services. Although most data was successfully committed to stable storage, some recently written data was lost due to power failures. It affected a tiny percentage of the total disk space, but it was significant for those impacted.

Question 2

Score: **5/5**

What were the long-term impacts on the organization due to the incident? Select all that apply.

- [ ] Increased customer trust and satisfaction
- [x] Highlighted infrastructure vulnerabilities
  Correct. The incident highlighted vulnerabilities in Google's data center infrastructure, particularly in handling power failures caused by lightning strikes. ✓
- [x] Identified weaknesses in reliability measures
  Correct. The lightning strike incident revealed the weaknesses in the organization's reliability measures. Changes were needed to improve lightning protection services and backup power supplies. ✓
- [ ] Decreased operational efficiency

Correct. The incident highlighted vulnerabilities in Google's data center infrastructure, particularly in handling power failures caused by lightning strikes..
Correct. The lightning strike incident revealed the weaknesses in the organization's reliability measures. Changes were needed to improve lightning protection services and backup power supplies..
You selected all correct options!

Question 3

Score: **5/5**

Describe the impact of the incident on customer trust and outline the strategic actions the organization implemented to restore trust.

The incident negatively affected customer confidence in Google's reliability, as some VM instances experienced read/write failures and there was minor but real data loss. Although the amount lost was extremely small—less than 0.000001% of total disk storage—the disruption raised concerns about the resilience of Google's infrastructure. For those filing support tickets, trust depended heavily on Google's ability to provide clear communication and demonstrate accountability, making the company's response and transparency critical to maintaining customer trust.

Strategic Actions to Restore Trust

- **Rapid Incident Response:** Google's Persistent Disk SRE team quickly declared a major incident, and the Incident Commander coordinated recovery efforts while Ops Leads worked to restore power and systems. Their structured approach minimized downtime and reassured customers that the situation was under control.
- **Transparent Communication:** A Communications Lead provided regular updates to internal leadership, storage teams, external customers, and those who had submitted support tickets. This openness helped customers feel informed rather than left in the dark.
- **Accountability and Public Statement:** Google released an online statement taking full responsibility for the disruption. They explained the cause, admitted the vulnerability of certain recently written data, and issued a public apology to all affected customers.
- **Infrastructure Improvements:** To prevent future incidents, Google committed to strengthening its backup battery systems, enhancing resilience against repeated disruptions, and improving automated failover systems. These steps aimed to show customers that Google was actively learning from the event and investing in long-term reliability.

The incident reduced customer trust because VM disruptions and minor data loss raised concerns about Google's reliability. To restore trust, Google acted quickly by declaring a major incident, assigning an Incident Commander to coordinate recovery, and restoring power with minimal downtime. They provided transparent updates through a Communications Lead to both leadership and customers, issued a public apology while taking responsibility, and explained why certain data was unrecoverable. Finally, Google committed to infrastructure upgrades such as stronger backup batteries, improved failover systems, and enhanced datacenter resilience to prevent future incidents.

The response deserves full marks because it thoroughly explains the impact on customer trust and provides specific examples of strategic steps taken by Google. The student mentions the rapid incident response, transparent communication, public accountability, and infrastructure improvements, aligning well with the highest rubric criterion.

For further improvement, consider including more details about the specific roles of the GCE and Persistent Disk teams in the incident response, as well as any additional measures Google could implement to enhance customer trust in the future.

Score: 5/5 (100%)

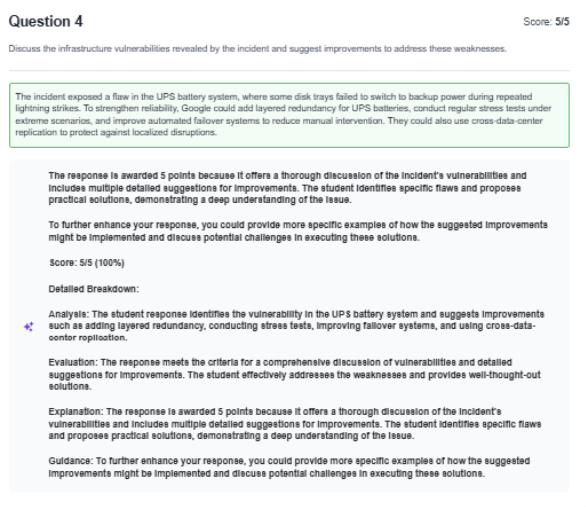
Detailed Breakdown:

Analysis: The student response provides a detailed analysis of the incident's impact on customer trust, noting the VM disruptions and minor data loss, and how these raised concerns about Google's reliability. The response also outlines strategic actions taken by Google, including rapid incident response, transparent communication, accountability, and infrastructure improvements.

Evaluation: The response meets the highest level of the rubric criteria by offering a thorough explanation of the impact on customer trust and detailing strategic steps to restore it. The student mentions specific actions like the declaration of a major incident, communication strategies, public accountability, and infrastructure improvements.

Explanation: The response deserves full marks because it thoroughly explains the impact on customer trust and provides specific examples of strategic steps taken by Google. The student mentions the rapid incident response, transparent communication, public accountability, and infrastructure improvements, aligning well with the highest rubric criterion.

Guidance: For further improvement, consider including more details about the specific roles of the GCE and Persistent Disk teams in the incident response, as well as any additional measures Google could implement to enhance customer trust in the future.



Question 4

Score: 5/5

Discuss the infrastructure vulnerabilities revealed by the incident and suggest improvements to address these weaknesses.

The incident exposed a flaw in the UPS battery system, where some disk trays failed to switch to backup power during repeated lightning strikes. To strengthen reliability, Google could add layered redundancy for UPS batteries, conduct regular stress tests under extreme scenarios, and improve automated failover systems to reduce manual intervention. They could also use cross-data-center replication to protect against localized disruptions.

The response is awarded 5 points because it offers a thorough discussion of the incident's vulnerabilities and includes multiple detailed suggestions for improvements. The student identifies specific flaws and proposes practical solutions, demonstrating a deep understanding of the issue.

To further enhance your response, you could provide more specific examples of how the suggested improvements might be implemented and discuss potential challenges in executing these solutions.

Score: 5/5 (100%)

Detailed Breakdown:

Analysis: The student response identifies the vulnerability in the UPS battery system and suggests improvements such as adding layered redundancy, conducting stress tests, improving failover systems, and using cross-data-center replication.

Evaluation: The response meets the criteria for a comprehensive discussion of vulnerabilities and detailed suggestions for improvements. The student effectively addresses the weaknesses and provides well-thought-out solutions.

Explanation: The response is awarded 5 points because it offers a thorough discussion of the incident's vulnerabilities and includes multiple detailed suggestions for improvements. The student identifies specific flaws and proposes practical solutions, demonstrating a deep understanding of the issue.

Guidance: To further enhance your response, you could provide more specific examples of how the suggested improvements might be implemented and discuss potential challenges in executing these solutions.

Question 5

Score: **5/5**

Case Study: Lightning Strikes Case Study (Part B)

Lessons Learned

o The importance of continual monitoring and maintenance of critical systems to prevent potential vulnerabilities.
o Timely intervention and proactive measures can significantly mitigate the impact of incidents.
o Regular testing and evaluating backup systems and battery backup capacity are essential to ensure data integrity and system reliability.
o Effective incident management and leadership are crucial in addressing complex situations.

Recommendations for Future Actions

o Conduct regular audits and assessments of critical systems to identify and address potential vulnerabilities.
o Implement automated monitoring systems to detect and address power-related issues promptly.
o Review and enhance battery backup systems to ensure adequate capacity and minimize the risk of extended or repeated battery drain.

Conclusion

The power failure incident at the data center was a valuable learning experience. It highlighted the importance of robust infrastructure, proactive maintenance, timely intervention, and effective leadership in ensuring the reliability and resilience of critical systems. Implementing the recommended actions and continuously improving infrastructure and processes can improve the organization's ability to provide uninterrupted and reliable services in the future.

Question 5: Which of the following are the key lessons learned from the lightning incident at the Google data center? Select all that apply.

- [x] The importance of continual monitoring and maintenance of critical systems. ✓
  Correct! Continual monitoring and maintenance are crucial to prevent vulnerabilities.
- [x] The significance of timely intervention and proactive measures. ✓
  Correct! Timely intervention can significantly mitigate the impact of incidents.
- [x] The necessity of regular testing and evaluating backup systems. ✓
  Correct! Regular testing ensures data integrity and system reliability.
- [ ] The need for increasing the number of data centers.

Correct! Continual monitoring and maintenance are crucial to prevent vulnerabilities..
Correct! Timely intervention can significantly mitigate the impact of incidents..
Correct! Regular testing ensures data integrity and system reliability..
You selected all correct options!

Summary

This activity analyzed Google's incident response to a series of lightning strikes that disrupted power at its Belgium data center in 2015. The strikes caused temporary storage

outages and minor data loss affecting Google Compute Engine virtual machines. The Persistent Disk SRE team declared a major incident, coordinated recovery, and provided transparent communication to stakeholders and customers. Google later issued a public statement, took responsibility, and committed to infrastructure improvements such as stronger backup systems and automated failover. The case study highlights the importance of redundancy, proactive monitoring, and clear communication in maintaining trust and resilience during unexpected disruptions.