ISSN: 1935-8156 Volume 19, Number 1, 2024, pp. 35-49 DOI: 10.3194/1935-8156-19.1.35

Security Considerations for Implementing Accounting Processes in the Cloud

Arti Mann
University of Northern Iowa, arti.mann@uni.edu

Abstract

This manuscript is a hands-on teaching case that places students in the role of an accounting consultant and helps them learn about the security issues at various levels of an accounting process implemented in the cloud. The students review the cloud-implemented accounting process in the context of accounting and security controls (COBIT and COSO ERM frameworks). They use cloud security architectures and models to prevent data leakage and to minimize or eliminate threats. General controls, IT controls, cloud implementation, and security are all topics typically taught in Accounting Information Systems (AIS) and audit courses. Instructors can use this case for an in-class discussion or out-of-class assignment.

Keywords
Cloud, information systems security, COBIT, COSO ERM

Acknowledgements
I extend my heartfelt gratitude to Betsy Haywood-Sullivan and Lorraine S. Lee, senior editors of the *AIS Educator Journal*, for their exceptional guidance and unwavering support, which were invaluable in bringing this case study to fruition. I also sincerely appreciate the reviewers for their insightful comments and constructive feedback, which significantly enhanced the quality of this manuscript.

Additionally, I would like to acknowledge the team at Theseus Data Lake (TDL) for their valuable assistance in exploring real-world implementation scenarios within large-scale global enterprises. Their expertise and contributions greatly enriched this study.

Cloud computing is becoming integral to every business because of the proliferation of remote work, geographically distributed teams, and specialization in certain aspects of business process outsourcing. Firms rely on having their business processes and systems housed in the cloud so that they are accessible from anywhere, provide a high degree of business continuity during natural disasters and localized outages, and promote lower TCO (total cost of ownership) in many cases (Alhomdy et al., 2021). According to a recent study by Gartner, by 2025, 51% of IT spending on application software, infrastructure software, business process services, and system infrastructure will have shifted from traditional solutions to public cloud solutions (Gartner, 2022).

Migration to the cloud allows organizations to centralize business processes and leverage integration between disparate systems. Centralization and integration lead to increased data velocity among data silos, system-generated audit trails, and locked-down security policies, which can be centrally implemented and monitored. This leads to reducing and/or eliminating data leakage, subverting system functions, and improving user experience to execute business processes in the cloud (Blue Prism, 2022).

Accounting practitioners must understand this emerging paradigm of cloud computing to drive business value and focus on decision-making. For small and medium-large firms, cloud computing and managing data are among the top 10 IT skills accountants need (Weisenfeld, 2020). This is also reflected in the AACSB Accounting Accreditation Standard, Standard A5: "Consistent with the mission, expected outcomes, and supporting strategies, accounting degree programs include learning experiences that develop skills and knowledge related to the integration of information technology in accounting and business. This includes the ability of both faculty and students to adapt to emerging technologies as well as the mastery of current technology" (AACSB, 2018, p. 22). This standard provides direction for accounting degree programs to integrate current and emerging accounting and business practices into three primary components within the curricula: information systems and business processes, data analytics, and technology agility among learners (AACSB, 2018).

The Information System and Controls (ISC) section of the Uniform CPA examination also reflects the importance of understanding cloud implementation, data management, and security (AICPA, 2022). This section details the skills CPAs must demonstrate regarding information systems, including security, privacy, and confidentiality. Topics included under areas 1 and 2 of the ISC exam are cloud computing, cloud deployment models, cloud service models, COSO framework for cloud computing governance, identifying and classifying different threats, data validation and verification, appropriate identification, and authentication techniques. This case covers many of these topics and provides an opportunity for students to analyze security and accounting controls for an accounting process in the cloud.

The case is based on a real-world implementation of a cloud-implemented accounting process for a global wealth management fund. The teams managing the operational cycles, including the technology, accounting, valuation, and cash management teams, provided much of the data and information necessary to create the case. The case provides an actual scenario that future audit/advisory staff may encounter. Additionally, it allows students to analyze security and accounting controls for an end-to-end mission-critical accounting process. This case uses the guidelines of security reference architectures from cloud service providers in the industry (e.g., Microsoft Azure, Amazon-AWS, CISCO, Google-GCP, and Oracle). These architectures provide a structure for understanding the security issues that can arise at various levels of accounting process implementation.

Literature Review

Risks in the current business environment, such as the 2008 financial crisis or the 2020 COVID-19 pandemic, are growing in complexity and volume, evolving in areas such as cybersecurity threats, economic fluctuations, and external risk events. Organizations using cloud computing face operational, reporting, and compliance risks (Lanz & Nearon, 2022) because their systems depend on nodes within and outside of their organization (Vohradsky, 2019). Substantial threats to cloud security include abuse and nefarious use, vulnerable security and application programming interfaces, data loss or leakage, unknown risk profiles, and inadequate infrastructure design and planning (Wlosinski, 2015). Attacks at the network and application levels can compromise an organization's information's confidentiality, integrity, and availability (De Donno et al., 2019).

Indeed, risks associated with cloud computing are disruptive in nature but not fully understood (Church et al., 2020). These risks highlight the need for mature Enterprise Risk Management (ERM) practices to help organizations manage their response to strategic, operational, and technology risks. Governance demands human intervention with automated processes through the identification of proper controls to mitigate these risks (Vohradsky, 2019). Mackita et al. (2019) and Lanz and Nearon (2022) stress the urgency of addressing enterprise risk management in a cloud computing environment. Mackita et al. (2019) note that major breakdowns in cloud computing functionality stemmed from organizations failing to properly identify, assess, and mitigate risks. Such protocols need to be conducted routinely. They combine elements of the COSO ERM model (2004) and an evaluation method for risk-

based security called OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). While they conclude that their approach provides effective risk management for cloud computing, they employ a framework that is now outdated. COSO updated its ERM model in 2017 to reflect strategic and operational aspects of business risk. Such perspectives are crucial in cloud computing, as evidenced by Grob and Cheng (2021).

In 2021, COSO commissioned a paper related to guidance on how the new COSO ERM framework applies to a cloud computing environment (Grob & Cheng, 2021). The authors walk through the 2017 COSO ERM principles and explain activities relating to cloud computing ERM. Grob and Cheng (2021, p. 25) emphasize the importance of considering risks in a cloud environment, writing: "Cloud computing risks must be identified and managed in the context of the organization's broader ERM program. While tasks, processes, and maintenance can be outsourced, accountability for risks cannot."

This case uses well-established frameworks—COSO ERM (2017) and COBIT 2019 (ISACA, 2018a; ISACA, 2018b; ISACA 2019)—which can be implemented at various levels of process automation to help mitigate cloud computing risks. Although these frameworks provide useful guidance to organizations, very few cases exist that require students to apply these frameworks to real-world situations. Cereola and Cereola (2011) ask students to evaluate the computer breach at TJX using earlier versions of the COSO ERM and COBIT frameworks. In Haywood (2021), students examine COBIT 2019 principles to demonstrate the vulnerabilities of IT Governance at a community college. In Haywood-Sullivan (2022), students analyze the principles and components of the 2017 COSO ERM framework to analyze the breakdown of enterprise-wide risks at Wells Fargo from 2009 to 2016.

Interestingly, there are even fewer cases that explore process implementation in the cloud. One case study (Gao, 2020) presents a content analysis approach to understanding and analyzing cloud ERP providers' data processing agreements. The case allows students to explore cloud ERP providers' data disclosure, security, sub-processing, and data retention and deletion practices. Another study (Alslihat et al., 2018) evaluates the impact of internal control components of the COSO framework on reducing the risk of cloud computing. These authors evaluate the accountant's perception of COSO's internal control framework for reducing the risk of cloud computing in Jordanian public shareholding companies, advocating for a deeper comprehension of the infrastructure and the provision of essential resources in information technology and skills. They propose the development of educational and training initiatives to equip auditors with knowledge of cloud accounting and its associated risks.

Many organizations provide guidance on security assessment, authorization, governance, and monitoring of cloud products and services, such as the Federal Risk and Authorization Management Program (FedRAMP), the National Institute of Standards and Technology (NIST), and the Cloud Security Alliance (CSA). However, no generic security architecture frameworks / models are available that can facilitate understanding the security issues related to implementing accounting processes in the cloud. This case (presented in Appendix A) fills this gap and provides information about the essential security components that must be considered while implementing an accounting process in the cloud. It also provides a structure for understanding the security issues that can arise at various levels of an accounting process implementation in the cloud. The case uses multiple security reference architectures from cloud service providers in the industry (such as Microsoft Azure, Amazon-AWS, CISCO, Google-GCP, and Oracle) in order to create a frame of reference. The details of these security reference architectures are provided in Appendix B.

Learning Objectives

This case aims to educate students about holistic IT security risk from the perspective of implementing applications in the cloud. In addition, the case allows students to leverage their pre-existing knowledge of the COSO ERM and COBIT (DSS: deliver, service, and support) frameworks. Furthermore, this case provides students an opportunity to analyze security and accounting controls for an end-to-end mission-critical accounting process. The specific learning objectives of this case are as follows:

- Students will learn about potential security considerations and external threats and compromises when implementing or migrating applications in a cloud environment.
- Students will assess risks and governance issues as they relate to accounting processes.
- Students will learn about the need for data selection and validation and IT audit controls related to cloud implementations of accounting systems.

Case Background

The case focuses on the service layer of the cloud security architecture. The service layer outlined in this case captures all the physical and logical layers that data travel through as it moves between users and systems.

Enterprise data may originate initially from various sources, including but not limited to ERP systems, legacy systems, historical data sources like archives, and long-term storage. Before the data is loaded into the target system, it must be cleaned, run through business rules for validation, and checked for errors and omissions (Romney & Steinbart, 2020; ISACA, 2018a, DSS06; COSO, 2020). Since enterprise data can also be loaded in machine-readable formats from external systems (XML), it must be scanned for malicious code and other attack vectors like SQL injection attacks (Halfond et al., 2006).

Edge and networking components of the service layer encapsulate the movement of data from the outer layers of a network (edge services) where external host systems are referenced and accessed using authenticated and known IT infrastructure services like a Domain Name System (DNS) and firewalls (ISACA 2018a, DSS05; COSO, 2020). Once past the edge, data is subject to additional checks via integration services like Extract Transform Load (ETL) and cross-platform validation, authentication, and validation (ISACA, 2018a, DSS05; COSO, 2020). Data may end up hosted in different storage silos segregated by origin, type, and target usage. This is achieved by the data and storage (including information protection) components of the service layer. Voluminous data may end up in a data warehouse; relational data would be stored in a structured relational database; and data made available in documents, media files, or other non-structured formats may end up being stored for later presentation in a content management system or document management system. At this stage, to avoid data loss due to unforeseen circumstances, data would also be copied to different data stores.

Depending on the criticality or sensitivity of the data, data may also be copied to different geographical locations to mitigate natural disasters (ISACA 2018a, DSS04 & DSS06; Romney & Steinbart, 2020). Legal and compliance requirements and regulations like the Sarbanes-Oxley Act may also dictate that data be made permanently available for a certain period. Organizations typically store such data in low-cost but secure storage, like encrypted backup tapes stored in off-site storage locations. Once the data is authenticated, it is validated, checked for errors, and made available in storage.

The next component of the service layer, processing and analytics, performs further operations on the data to make it available for consumption by users and other systems as well as additional classification and categorization (ISACA 2018a, DSS06). This is typically achieved by tagging the data with metadata markers, handing it off to content delivery networks, and presenting it visually via dashboards. This is done while capturing and monitoring the quality-of-service metrics to ensure data velocity is maintained so that data is presented promptly and consistently with an organization's internal guidelines. The analytics component makes the data available for further analysis and reporting. Analytics services may also transform the data into other formats for consumption by other systems for reporting and visualization.

Case Description

In this case scenario, the students take on the role of a consultant who has been hired to review the potential risks of the invoice processing and payment process of the Global Investment Fund (GIF). The students must review appropriate accounting and security controls across the entire application to ensure the prevention of fraudulent payments and potential compromises of the DLM (Data Lifecycle Management) process. The students review the process roadmap in the context of data security, accounting control, monitoring, and the potential of external threat vectors like intrusion by malicious actors. Furthermore, students analyze the possibility of introducing additional accounting controls to ensure the process meets compliance and data-governance requirements. For reference, in addition to coverage at varying lengths in other AIS textbooks, these materials are covered in Romney and Steinbart (2020):

- Chapter 10: Control and Accounting Information Systems—control frameworks; assess and respond to risk using ERM model; control activities commonly used in companies
- Chapter 11: Controls for Information Security—fundamental information security concepts; understanding targeted attacks; preventive controls; detective controls; corrective controls; security implications of virtualizations and the cloud
- Chapter 12: Confidentiality and Privacy Controls—preserving confidentiality; encryption
- Chapter 13: Processing Integrity and Availability Controls—processing integrity; availability

To complete this case, the students have an accounting process roadmap (Figure A1) that has been implemented in the cloud. The students must review the material and the diagram provided to assess which COBIT 2019 or

COSO ERM standards would be suitable to ensure data integrity as information flows across the accounting process. Using the cloud security guidelines in Appendix B, the students must also assess the potential vulnerabilities of process steps from a security perspective.

Implementation Guidance

Courses that could incorporate the case include Accounting Information Systems (AIS) and IT audit undergraduate or graduate courses. Before introducing this case, the instructor should cover the topics of IT controls, control frameworks, and controls for information security. To go more in depth, the instructor may want to cover the different modes of deployment of the cloud (public, hybrid, and private cloud), the importance of information security irrespective of the traditional implementation or cloud implementation, specific domains of COSO ERM and COBIT 2019 frameworks (as described in Appendix C), expenditure controls, governance, and compliance controls to maintain data integrity in accounting applications and processes. If emerging technologies have not been covered before this case, the instructor could introduce the concept of cloud computing, including definitions, cloud service models (SaaS, PaaS, IaaS), and deployment models. This material, as well as recommended resources, is provided in Appendix B.

After covering the topics, the instructor can introduce the actual case scenario (Figure A1) and the assignment (Appendix A). Students then complete the case and submit a file with the answers to the questions. In a subsequent class, the instructor can review the correct solutions and generate classroom discussion on the various approaches students used to develop their answers.

This case is intended to be completed in groups. It is set up this way because cloud security is a complicated topic, and students will benefit from discussions with each other. In their groups, students should be able to complete the case in 1 hour 15 minutes. However, if the instructor assigns the case individually, the instructor should allocate more time (approximately 2 hours).

The instructor can implement the case in two ways: 1) the teaching and assignment are both done in class, and 2) the teaching is done in class, and students complete the assignment outside of class. If the assignment is to be done in class and the instructor wants to be efficient with class time, this person may distribute resources on the preparatory topics with students ahead of class coverage.

Two professors reviewed the case for its efficacy and relevance in achieving its stated learning objectives and its realism to current professional environments. One professor, who reviewed the case, plans to use the case in a graduate-level internal audit class in the future and suggested discussing the Trust Services Framework—security, privacy, confidentiality, processing integrity, and availability (AICPA & CIMA, 2017) prior to working the case. Another professor who reviewed the case suggested the following approach for implementation:

a) For undergraduate students, use the case over several class sessions that cover COSO/COBIT and IT controls. Introduce the case earlier and use authentic assessment (Wiggins, 2019). Wiggins describes assessment as authentic when we directly examine student performance on worthy individual tasks. He further adds, "Authentic tasks involve 'ill-structured' challenges and roles that help students rehearse for the complex ambiguities of the 'game' of adult and professional life. Traditional tests are more like drills, assessing static and too-often arbitrarily discrete or simplistic elements of those activities" (Wiggins, 2019, p. 2). Because this case allows students to learn through writing, revision, and discussion in the second part of the case (the assignment part), authentic assessment would work well here. Implementing this case over several weeks will allow for that and, through authentic assessment, provide more clarity in learning IT controls, which is essential for accountants in the workplace.
b) For graduate students, the instructor could use the case in class and have them complete a reflective writing assignment specific to the case, focusing on the importance of security, the understanding of threats, and the need for controls.

Furthermore, the two professors who reviewed this case expressed interest in utilizing it for undergraduate and graduate AIS and audit classes. One professor highlighted the case's value in reviewing IT governance principles.

Case Efficacy

The usefulness of the case was evaluated in Fall 2023 in an undergraduate AIS course at a southwestern university. Thirty students completed the assignment in class. Students were surveyed after the case assignment was completed to assess student perceptions of the case. The survey questions were adopted from Lee and Sawyer (2019).

Table 1
Student Perceptions[a]

	Questions	N = 30	STDEV
Q1	This case helped me understand the need for and importance of security for accounting applications in the cloud.	5.90	0.98
Q2	I understand better how different stakeholders (business managers, accountants, cash managers) can use common platforms to execute a business process.	5.30	1.16
Q3	The case was a positive learning experience.	5.87	1.26
Q4	I understand the nature and type of security compromises that may be used to target cloud platforms.	5.50	0.81
Q5	I understand the importance of accounting controls in cloud applications for financial transactions.	6.20	0.87
Q6	This case helped me understand the importance of COBIT / COSO ERM standards for application controls.	5.13	1.31
Q7	This case was an interesting case assignment.	5.60	1.25
Q8	This case will be useful for future accounting undergraduate students.	6.03	0.98
Q9	I recommend continuing to use this case with undergraduate accounting students.	5.90	1.11
Q10	I understand the need for and importance of governance controls in accounting applications.	6.23	0.72

[a]Scale: 1 = Strongly Disagree; 2 = Disagree; 3 = Slightly Disagree; 4= Neither Agree nor Disagree; 5 = Slightly Agree; 6 = Agree; 7 = Strongly Agree

Students responded positively to the case, agreeing that the case helped them learn the importance of cloud security and the nature and types of security compromises (i.e., Q1 mean score: 5.90; Q4 mean score: 5.50). Notably, the respondents agreed that the case would be useful to future accounting undergraduate students (Q8 mean score: 6.03) and recommended continual usage of the case (Q9 mean score: 5.90).

The instructor who assigned the case was pleased with the student outcomes. The instructor shared three learning objectives with the class to assess the outcomes and provided a reflective learning assignment. Students mentioned a new awareness of the importance of security, the understanding of threats, and the need for controls. While this case was implemented with undergraduate students in an AIS class, the core focus of the case related to IT security and cloud implementation, which are topics that are also appropriate for the graduate-level IT audit class.

Conclusion

Overall, this case allows students to understand IT security from the perspective of implementing applications in the cloud and provides an exercise where students can apply their knowledge of COBIT and COSO ERM frameworks. The case also allows instructors to emphasize the importance of IT and accounting controls.

References

AACSB. (2018). *AACSB accounting accreditation standards*. https://www.aacsb.edu/educators/accreditation/accounting-accreditation/aacsb-accounting-accreditation-standards.

AICPA. (2022). *Uniform CPA examination blueprints*. December 1, 2022.

AICPA & CIMA. (2017). *Trusted services framework* https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022

Alhomdy, S., Thabit, F., Abdulrazzak, F. H., Haldorai, A., & Jagtap, S. (2021). The role of cloud computing technology: A savior to fight the lockdown in COVID-19 crisis, the benefits, characteristics, and applications. *International Journal of Intelligent Networks*, *2*, 166–174. https://doi.org/10.1016/j.ijin.2021.08.001

Alslihat, N., Matarneh, A. J., Moneim, U. A., Alali, H., & Al-Rawashedh, N. H. (2018). The impact of internal control system components of the COSO model in reducing the risk of cloud computing: The case of public shareholding companies. *Ciência E Técnica Vitivinícola*, *33*(4), 188–202.

Blue Prism. (2022). *5 reasons why you should deploy RPA in the cloud.* https://www.blueprism.com/resources/white-papers/5-reasons-why-business-leaders-are-deploying-cloud-rpa-and-ia/

Cereola, S. J., & Cereola, R. J. (2011). Breach of data at TJX: An instructional case used to study COSO and COBIT, with a focus on computer controls, data security, and privacy legislation. *Issues in Accounting Education*, *26*(3), 521–545. https://doi.org/10.2308/iace-50031

Church, K. S., Schmidt, P. J., & Ajayi, K. (2020). Forecast cloudy—fair or stormy weather: Cloud computing insights and issues. *Journal of Information Systems*, *34*(2), 23–46. https://doi.org/10.2308/isys-18-037

Cisco. (2023). *Cisco security reference architecture*. https://www.cisco.com/c/en/us/products/security/cisco-security-reference-architecture.html#~overview

COSO. (2017). *Enterprise risk management: Integration with strategy and performance*. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

COSO. (2020). *Compliance risk management: Applying the COSO ERM framework*. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf

De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. *Future Internet*, *11*(6), 127. https://doi.org/10.3390/fi11060127

Gao, L. (2020). Exploring the data processing practices of cloud ERP—a case study. *Journal of Emerging Technologies in Accounting*, *17*(1), 63–70. https://doi.org/10.2308/jeta-52680

Gartner. (2022). *Gartner says more than half of Enterprise IT spending in key market segments will shift to cloud by 2025*. https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

Grob, M., & Cheng, V. (2021). *Enterprise risk management for cloud computing*. Committee of Sponsoring Organizations of the Treadway Commission. https://riskcue.id/uploads/ebook/20211227102445-2021-12-27ebook102433.pdf

Halfond, W. G. J., Viegas, J., & Orso, A. (March 13-15, 2006). A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering*, *1*, 13–15.

Haywood, M. E. (2021). Making the grade: Using COBIT to study computer crime at Bucks County Community College (Pennsylvania). *Journal of Information Systems Education*, *32*(2), 115–118.

Haywood-Sullivan, B. (2022). Using the 2017 COSO ERM framework to examine risks at Wells Fargo. *AIS Educator Journal*, *17*(1), 9–17. https://doi.org/10.3194/1935-8156-17.1.9

ISACA. (2019). *Effective IT governance at your fingertips*. https://www.isaca.org/resources/cobit

ISACA. (2018a). *COBIT 2019 framework: Governance and management objectives*.

ISACA. (2018b). *COBIT 2019 framework: Introduction and methodology*.

Lanz, J., & Nearon, B. (2022). Risk impacts of SaaS cloud computing. *The CPA Journal*, *92*(7–8), 52–57. https://www.cpajournal.com/2022/10/05/risk-impacts-of-saas-cloud-computing/

Lee, L., & Sawyer, R. (2019). IT general controls testing: Assessing the effectiveness of user access management. *AIS Educator Journal*, *14*(1), 15–34. https://doi.org/10.3194/1935-8156-14.1.15

Mackita, M., Shin, S., & Choe, T. (2019). Ermoctave: A risk management framework for IT systems which adopt cloud computing. *Future Internet*, *11*(9), 195. https://doi.org/10.3390/fi11090195

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology, U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Microsoft. (2021). *Microsoft cyber security reference architecture*. Retrieved July 1, 2023, from https://learn.microsoft.com/en-us/security/cybersecurity-reference-architect20ure/mcra

Oracle. (2024). *Oracle Cloud Infrastructure Security Architecture*. https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

Romney, M. B., & Steinbart, P. J. (2020). *Accounting information systems* (15th ed.). Pearson Education, Inc.

Vohradsky, D. (2019). A model and best practices for risk transformation. *ISACA Journal*, *3*, 1–12. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-3/a-model-and-best-practices-for-risk-transformation_joa_eng_0519.pdf

Weisenfeld, L., Mathiyalakan, S., & Heilman, G. (2020). Topics for your undergraduate accounting information systems (AIS) course—an exploratory study of information technology (IT) skills and firm size. *AIS Educator Journal*, *15*(1), 58–89. https://doi.org/10.3194/1935-8156-15.1.58

Wiggins, G. (2019). The case for authentic assessment. *Practical Assessment, Research, & Evaluation*, *2*(2). https://rpgroup.org/Portals/0/Documents/Projects/BRIC/The%20Case%20for%20Authentic%20Assessment%20-%20Wiggins.pdf

Wlosinski, L. G. (2015). Cloud insecurities. *ISACA Journal*, *2*, 1–5. https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/cloud-insecurities

Zhang, C., Issa, H., Rozario, A., & Soegaard, J. S. (2023). Robotic process automation (RPA) implementation case studies in accounting: A beginning to end perspective. *Accounting Horizons*, *37*(1), 193–217. https://doi.org/10.2308/HORIZONS-2021-084

Appendix A

The Case

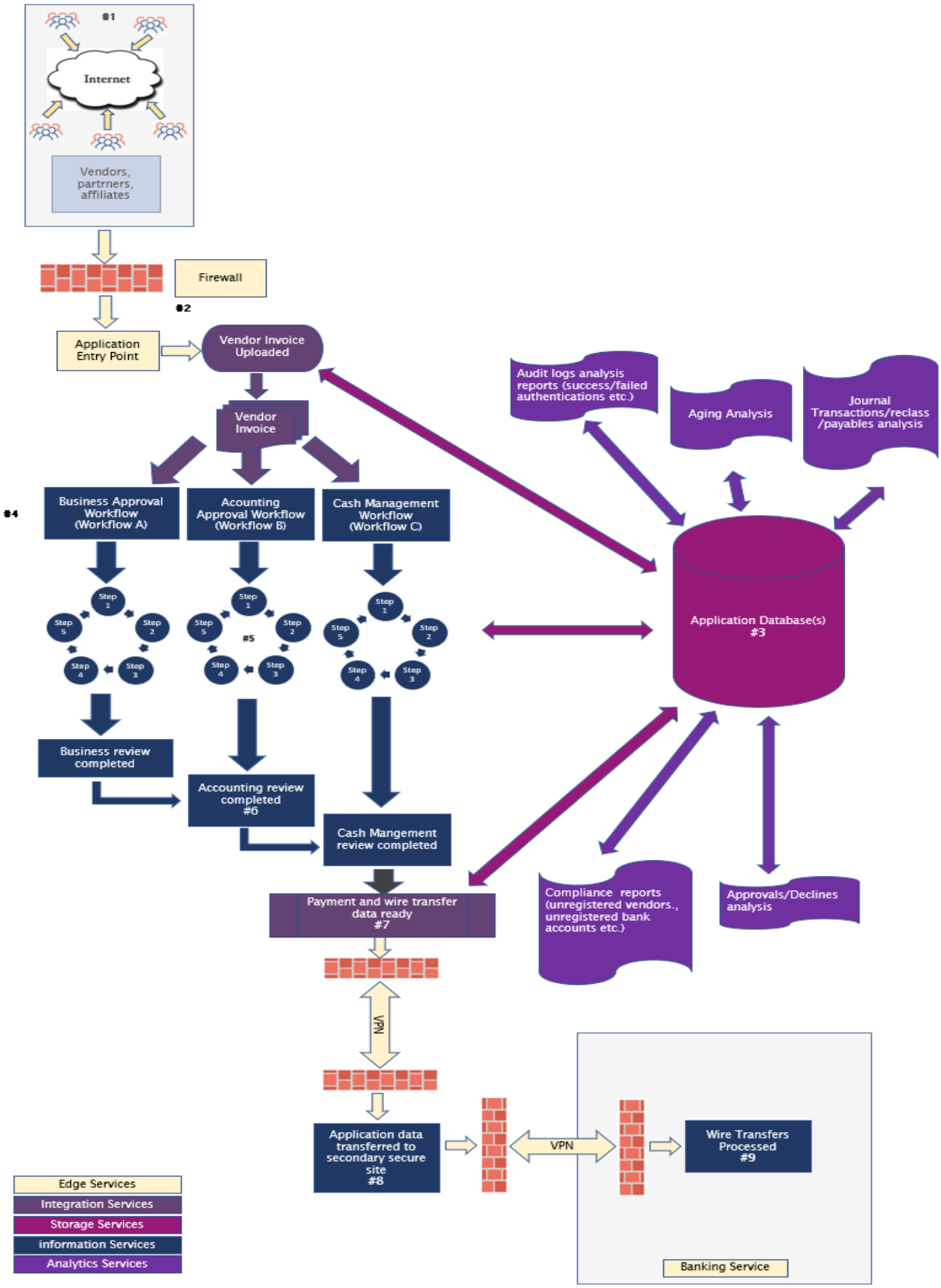
GIF (Global Investment Fund) is a large global fund with real estate investments and assets in multiple countries in the world. GIF works with hundreds of vendors, affiliates, and partners on investment projects in every country in which they operate. These vendors submit thousands of invoices monthly by email for approval and payment processing. Some invoices are generated electronically using their billing systems, some are sent as PDF files, and many are paper-based invoices.

GIF managers must review and approve all invoices. Once approved, the accounting team processes the invoices for payments and instructs the treasury team to make the wire transfers for each invoice on the payment date. The treasury team has to manually perform wire transfers to pay each invoice, while ensuring that the vendors and payment information listed on every invoice belongs to an approved project or task and the vendor is authorized to do business with the GIF. At the end of each month, each country's branch processes its financial statements according to the country's own accounting standards. The local books are then consolidated into the global U.S.–based financial statements while adjusting for International Financial Reporting Standards (IFRS) (for reporting) as well as U.S. Generally Accepted Accounting Principles (GAAP) adjustments for U.S. regulatory compliance. This process is very time-consuming, error-prone, and labor-intensive.

The GIF is considering implementing a global cloud-based platform/application that performs the following functions. The cloud implementation would be a hybrid cloud (a mix of public as well as private cloud services). The step numbers correspond with the numbers in Figure A1.

1) The application is accessible from every country the GIF operates in and is accessible to every vendor, partner, and affiliate.
2) The application has multi-layered security with access control based on MFA (multi-factor authentication), and access to every project is strictly controlled and provided only to those vendors who are part of that project. Vendors must be able to view only the data to which they have access.
3) The application must implement a global database of all vendors, partners, and affiliates with their banking information. Vendors and their banking information must be strictly controlled with multiple levels of approval required by the business managers and cash management / treasury teams.
4) The application allows the vendors to upload the invoices wherein they select to which investment (project or asset) it is related. The application then automatically kicks off a workflow to circulate the invoices for approval amongst the relevant stakeholders (see workflow A in Figure A1).
5) Parallel to step 4 above, the application also automatically and pre-emptively creates Accounts Payable journal entries and waits for accounting approval (see workflow B).
6) If invoices are not approved, the system reverses them outright.
7) In conjunction with step 6, the application also prepares wire transfer instructions for the bank while keeping the treasury team notified (see workflow C).
8) Once the treasury team has reviewed and approved, the application connects to the banking provider online and performs the wire transfers. The application selects the payment bank accounts that have been approved and onboarded within the application previously.
9) For security purposes, the banking functions must be performed in a private cloud with access allowed only from pre-approved and whitelisted IP addresses. GIF wants to implement this application following the principles of cloud security. GIF also wants to ensure all input/output processes and checks/validations are in place per guidelines such as COBIT and COSO ERM.

Figure A1
Payments Process Implementation in Cloud



You have been hired as a consultant to review the potential risks of GIF invoice processing and payment processing. You must review appropriate accounting and security controls across the entire application to prevent fraudulent payments and potential compromises of the DLM (Data Lifecycle Management) processes that may exist in the organization. The cloud security guidelines (the main components) and accounting automation process roadmap (Figure A1) have been color-coded to represent which guiding principle in the security architecture of the service layer corresponds with a particular process in the roadmap.

Instructions

1) In Figure A1, highlight the data-interchange points where data validation and verification are needed, and explain why.
2) Describe what standards from COBIT 2019 or COSO ERM 2017 would be best suited to ensure data integrity as it flows across the automated process within the application.
3) Referencing Figure A1, indicate whether the following vulnerabilities exist at each process step in the table below.

Table A1

Potential Vulnerabilities

Vulnerabilities	Process Steps (Figure A1)								
	#1	#2	#3	#4	#5	#6	#7	#8	#9
Misconfigured Access Control									
Broken Authentication / Second Factor									
Erroneous User Entitlements									
Confidential Data Leakage									
Executable File Upload									
Misconfigured / Lack of Input Control									
External Hacking									
Unauthorized Data Manipulation									
Internal Bad Actors (Insider Threats)									

4) In Figure A1, where can additional accounting controls be added, and how?
5) (Optional): Create a presentation for the client that outlines the potential risks associated with the cloud implementation of the Global Investment Fund (GIF) payment process. Present your assessment findings regarding accounting and security controls and subsequently discuss the potential security risks within the relevant layers of the implementation.

Appendix B

Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2).

Service Models

NIST defines three fundamental service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Mell & Grance, 2011).

- Software as a Service (SaaS): "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings" (p. 2).
- Platform as a Service (PaaS): "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment" (pp. 2–3).
- Infrastructure as a Service (IaaS): "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)" (p. 3).

Deployment Models

NIST defines four deployment models (p. 3):

- Public Cloud: "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."
- Private Cloud: "The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."
- Hybrid Cloud: "The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."
- Community Cloud: "The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."

Cloud Security Architectures and Models

Every large software, network infrastructure, and cloud service provider (such as Microsoft Azure, Amazon-AWS, CISCO, Google-GCP, and Oracle) publishes security reference architectures that guide customer implementations in the cloud and on the premises. These reference architectures aim to inform and educate an organization's network and application teams to safeguard organizational information assets, prevent intrusion by malicious third parties, and minimize data loss due to external threats. These architectures incorporate industry best practices and technology implementations to mitigate the overall risk of network intrusion, access compromise, data loss, and downtime. Implementing an architecture based on trust where information/data is not pre-validated/pre-verified can introduce security vulnerabilities, and a security vulnerability in one part of the architecture can compromise the rest of the implementation. The architectures are built on zero trust principles, which force network,

infrastructure, and application components to implement access control decisions based on explicit validation of user trust and endpoint integrity (Microsoft, 2021; Cisco, 2023; Oracle, 2024).

There are four broad layers in these architectures. These layers are:

- A Physical Network (underlying hardware)
- Virtual (virtual machines running specific operating systems and applications)
- Services (edge services, compute services, application-level assets like storage, networking, databases, etc.), and
- Governance.

Security architectures are modeled around these layers, based on end-user deliverable functions and specific feature sets. This case focuses on the services layer of these cloud security architectures and references the security architectures from Microsoft, Cisco, and Oracle (Microsoft, 2021; Cisco, 2023; Oracle, 2024).

The service layer consists of the following components (Oracle, 2024):

- Edge and Networking: This layer comprises of a combination of infrastructure and application deployments that enable connectivity to outside networks and services. It provides network traffic authentication and filtering, blocks external network attacks, and prioritizes legitimate network traffic streams. It is also responsible for maintaining QoS (Quality of Service) for network traffic and ensuring uptime and reliability by providing redundant layers to minimize disruptions.
- Database and Storage (Data and Information Protection): This houses all the data and information received, created, and generated as part of the business functions and processes. This layer ensures all data is stored and available for consumption by higher service layers, and it provides specific implementations driven by the type of data. It can store relational, multidimensional, unstructured, and any other type of data with meta-tagging to ensure data is available in the expected format as needed. This layer is also responsible for persisting data based on the classification in short-term or long-term data stores (server storage, backup storage, offline media like tapes, etc.) as mandated by data governance and eDiscovery policies and guidelines.
- Compute (Processing and Analytics): This layer is responsible for providing all the data processing and analytical services that act on the raw and processed data. It is responsible for running analytical and other processes to turn data into actionable information for decision-making or feeding it to other ancillary services to further act on them. It also applies information security policies when the type and nature of data and information changes due to data transformation services.

Appendix C

COBIT and COSO ERM Frameworks

COBIT and COSO ERM frameworks help create and manage internal controls for risk management and IT Governance. Both of these are companionable and highly synergistic. However, these frameworks differ in their purpose, scope, and level of detail.

COBIT

According to ISACA, governance and management objectives are requisites for effective enterprise management of information and technology. ISACA categorizes governance and management objectives of COBIT into five domains. Evaluate, Direct and Monitor (EDM) are the governance objectives which assist with strategic initiatives. The other four relate to management objectives. Align, Plan and Organize (APO) address organizational and supporting activities of information and technology. Build, Acquire and Implement (BAI) relate to the acquisition, implementation and integration of business processes. Deliver, Service and Support (DSS) focuses on the operational delivery, support and security of information and technology. Monitor, Evaluate and Assess (MEA) focuses on performance monitoring and conformance. (ISACA 2018b). While all are important, this case focuses on protecting enterprise information and business processes and maintaining security and controls to accomplish this. Therefore, DSS objectives are the most applicable, especially DSS04 (Managed Continuity), DSS05 (Managed Security Services) and DSS06 (Managed Business Process Controls). Key objectives and activities for these management objectives can be found in ISACA's *COBIT 2019 framework: Governance and management objectives*. This guidance can be downloaded for free at https://www.isaca.org/resources/cobit#2.

Once acquired, a focus should be on the management practice objectives and activities. For example, DSS04.01 (Define the business continuity policy, objectives and scope) improves business resilience through activities such as: identifying critical internal and outsourced business; recognizing key stakeholders to improve continuity policies; documenting policy objectives and scope; and identifying essential supporting business processes and related I&T services. By reviewing the detailed activities and relating them to the steps in Figure A1, students can thoughtfully consider the vulnerabilities that can occur at each stage.

COSO ERM

COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission. In 2017, COSO published "Enterprise Risk Management Framework: Integrating with Strategy and Performance," an updated framework for audit, risk, and compliance professionals to leverage in developing risk management plans. The framework defines enterprise risk management (ERM) as the "culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value" (p. 10). This framework explains how five areas (governance and culture; strategy and objective-setting; performance; review and revision; and information, communication, and reporting) interrelate to reduce risk and drive firm success. Performance is inherently tied to risk, per the COSO ERM guidelines. Five principles fall under the Performance component: identifies risk; assesses severity of risk; prioritizes risk; implements risk responses; and develops a portfolio view. Process risk identification, assessment, and management of risks by an automatic system application of business rules mitigates risks such as flagging fraudulent invoices and unregistered vendors. It also helps create an overall or "portfolio" view of the risks associated with the payables accounting process(es). Examples of specific considerations for cloud security under the Performance area are multi-tenacy, access controls and redundancy (Grob & Cheng, 2021). Moreover, when responding to risk with respect to cloud computing, Grob and Chen (2021) note that the most prominent action should be reduction. Grob and Cheng (2021, p. 19) summarize these risks and responses in their Table 3.2 (Summary of Common Cloud Computing Risks and Risk Responses), which can be accessed at: https://riskcue.id/uploads/ebook/20211227102445-2021-12-27ebook102433.pdf. This document may be useful for students in identifying vulnerabilities associated with processing in the cloud.

AIS Educator Journal Editorial Board 2023-2024

The AIS Educator Journal is published by the AIS Educator Association:
President: William G. Heninger, Brigham Young University
Vice President and President-elect: Gary P. Schneider, California State University, Monterey Bay
Secretary: Sonia Gantman, Bentley University
Treasurer: Kristian Mortenson, University of St. Thomas
Past-President: Ronald J. Daigle, Sam Houston State University