ISSN: 1935-8156 Volume 19, Number 1, 2024, pp. 50–69 DOI: 10.3194/1935-8156-19.1.50

The Sunday Standstill: An Accounting Information System Upgrade Role-Play

Randi Jiang
Grand Valley State University, jiangr@gvsu.edu

Meagan Luttenton-Knoll
Grand Valley State University, luttenme@gvsu.edu

Paul Hillman
Grand Valley State University, hillmanp@gvsu.edu

Daniel A. Pellathy
University of Tennessee, Knoxville, pellathy@utk.edu

Abstract

The role-play "The Sunday Standstill" bridges the gap between theoretical frameworks and real-world decision-making in accounting information systems (AIS). The role-play focuses on information security policy violations, internal control weaknesses, IT governance challenges using the COSO and COBIT frameworks, and the fraud triangle. This role-play is designed to achieve key learning goals, including strengthening students' understanding of information security deficiencies, risk assessment, internal controls, critical thinking, professional skepticism, and enhancing collaboration and communication skills. Unlike traditional case studies, this role-play fosters active decision-making in complex, ambiguous situations, preparing students for professional challenges. Students find this exercise both exciting and relevant. The role-play is appropriate for undergraduate accounting information systems, IT audit, and assurance types of courses.

Keywords
COSO internal control framework, COBIT framework, fraud triangle, internal controls, cybersecurity, AIS, management information systems, information systems risk assessment, role-play learning

Individuals significantly influence the effectiveness of their organizations' information and cybersecurity practices (Burns et al., 2018; Posey & Folger, 2020). Since the implementation of the Sarbanes-Oxley Act (SOX) of 2002, there has been an increased focus on training accountants to assess risk and strengthen internal controls, particularly those related to information systems.

To aid with the risk assessment of organizations, frameworks such as the control deficiency evaluation framework found in Auditing Standard No. 5 (AS5) of the Public Company Accounting Oversight Board (PCAOB), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the Control Objectives for Information and Related Technologies (COBIT) created by ISACA have been instrumental. These frameworks help companies create a strong culture of cybersecurity practices and effective information security policies (ISPs) to prevent and detect cybersecurity attacks (Bee et al., 2021; Haywood-Sullivan, 2022).

Despite these efforts, research has shown that employees are often the weakest link in information security (Bulgurcu et al., 2010; Martins & Elofe, 2002; Posey & Folger, 2020). Research also shows that high-stress conditions induce a tendency toward unethical behavior, such as ISP violations (Kouchaki & Desai, 2015; Selart & Johansen, 2011). These findings underscore the importance of integrating employee-focused strategies into risk management frameworks to address the human factors in cybersecurity more effectively.

A role-play is an active learning strategy that simulates real-world scenarios, allowing participants to assume specific roles and engage in interactions that mirror actual workplace situations. By placing students in these roles, role-play encourages critical thinking, problem-solving, and collaboration (Powell et al., 2020). Participants navigate complex situations, respond to challenges, and make decisions as their assigned characters, mimicking the dynamics of real-life decision-making in organizations.

In this paper, we develop a teaching case based on role-play that provides an interactive approach to engaging students with the challenges of ISP violations. The case uses the COSO and COBIT frameworks as tools for risk assessment (Lehmann & Hao, 2020). Specifically, students critically examine different interpretations of ISP violation behaviors through these frameworks, exploring their potential consequences for individuals and organizations. Because the role-play incorporates the fraud triangle's focus on motivation, opportunity, and rationalization, students gain a deeper understanding of the drivers behind noncompliant behavior.

This multifaceted approach equips students with a comprehensive perspective on internal controls, IT governance, and the ethical dimensions of security policy compliance.

The Role-Play Overview

The role-play "The Sunday Standstill" simulates real-world Information Technology (IT) governance and Accounting Information Systems challenges, enabling students to apply theoretical frameworks, assess risks, and propose solutions in a collaborative setting. Inspired by a real-life situation encountered by one of the authors, the scenario ensures authenticity in its design. To enhance its relevance for today's classrooms, the situation has been adapted to reflect modern challenges in information systems governance, cybersecurity threats, and Enterprise Resource Planning (ERP) systems. By integrating the COSO framework, COBIT framework, and the fraud triangle, the role-play provides a structured approach for students to evaluate internal controls, identify potential risks, and understand the motivations behind noncompliant behaviors.

In the role-play, a company hires a consulting firm to upgrade its outdated, disconnected accounting and manufacturing systems. The current system lacks integration, requires manual payroll processing, and has IT security vulnerabilities, including shared login credentials and unsupported software. The planned ERP upgrade, co-led by a senior consultant and the company's technology director, aims to unify systems, improve data integration, enhance security, and streamline payroll. The upgrade begins on Friday night and is intended to be finished by Monday morning. However, on Sunday, the process freezes, locking the old and new systems and stalling progress. The team faces a tense standstill with no technical support available until Monday.

As the role-play unfolds, individual character backstories add layers of detail and tension, enriching the scenario and deepening the challenges the team encounters. Unlike traditional case studies, which present static narratives, the scenario evolves dynamically, presenting unexpected challenges to simulate real-world complexities. Students are initially given broad, deliberately vague instructions, but new details emerge as the role-play progresses, creating unexpected twists. Like a "whodunit mystery," this scenario challenges students to apply their knowledge and problem-solving skills while adapting to evolving circumstances. This experience promotes collaboration and critical thinking, requiring students to embrace ambiguity and recognize that there may not be a single correct answer (Boyce et al., 2015).

The role-play also includes deliverables directly connecting to the course learning objectives. For instance, students apply COSO and COBIT principles to evaluate risks and propose controls while using the fraud triangle to

assess potential unethical behaviors. These deliverables challenge students to think critically about the implications of their decisions and propose actionable solutions grounded in applicable frameworks. Instructors have flexibility in how they implement the role-play. The activity can be adapted to fit different class sizes, learning objectives, and time constraints. This role-play can provide an innovative approach to accomplishing specific course requirements.

Student feedback consistently highlights the role-play as engaging and highly relevant, emphasizing its value in fostering collaboration, critical thinking, and practical skills. The role-play bridges the gap between academic learning and professional preparation by encouraging students to grapple with complex and ambiguous scenarios.

Learning Objectives

The role-play is designed to support a range of learning objectives, allowing instructors to select which objectives to emphasize without needing to modify the activity. By incorporating a dynamic scenario, character backstories, targeted deliverables, and guided discussions, the role-play promotes mastery of common AIS course objectives while fostering critical thinking through the application of key frameworks and concepts:

- COBIT Framework Analysis
  Analyze the ERP failure, focusing on:
  - Governance: Improve IT governance considering leadership challenges.
  - Risk Management: Address credential and communication risks.
  - Compliance: Emphasize protocol adherence to prevent future issues.

  Outcome: Enhance students' ability to think critically about COBIT domains and their applications for governance and compliance.
- COSO Framework Evaluation
  Evaluate the ERP failure with COSO to identify weaknesses, focusing on:
  - Internal Controls: Examine how gaps contributed to ERP and payroll issues.
  - Risk Assessment: Identify risks from oversight and communication gaps.
  - Control Activities: Propose activities to enhance monitoring and fraud detection.

  Outcome: Strengthen skills in applying COSO for internal controls and accountability.
- Fraud Triangle Analysis
  Analyze actions in the case using the fraud triangle, focusing on:
  - Fraud Elements: Explore opportunity, pressure, and rationalization in fraud.
  - Motivations: Investigate pressures leading to unethical behavior.
  - Mitigation Strategies: Develop strategies to reduce fraud opportunities.

  Outcome: Encourage critical evaluation of fraud scenarios and effective strategies for mitigating unethical behavior.
- Shadow IT Implications
  Explore risks and governance for unauthorized IT use, focusing on:
  - Instances of Shadow IT: Identify and document unauthorized software use.
  - Risk Analysis: Assess risks like data breaches and compliance issues.
  - Governance Framework: Propose policies for monitoring shadow IT.

  Outcome: Understand shadow IT risks and governance for IT resource management.
- Ghost Employees and Payroll Fraud
  Identify and address ghost employee risks, focusing on:
  - Occurrences: Document instances of ghost employees.
  - Financial & Ethical Impact: Evaluate financial losses and ethical implications.
  - Prevention Strategy: Develop audits and reports for accountability.

  Outcome: Recognize payroll fraud risks and the importance of robust controls.
- Information Security Policy (ISP) Review
  Assess and enhance Blue House's ISP, focusing on:
  - Best Practice Alignment: Compare ISP against industry standards (NIST, ISO).
  - Vulnerability Identification: Identify gaps in access controls and data security.
  - Enhancements: Recommend updates, training, and incident response measures.

  Outcome: Build an understanding of effective ISP in safeguarding organizational data.

The objectives listed can be adjusted to fit the needs of individual courses. Omitting or modifying the number of objectives will not change the scenario or the backstories. The scenario (Appendix A) and backstories (Appendix B) are designed to allow students to either focus on or overlook specific details, depending on the assigned deliverables.

Prerequisite Knowledge and Skills

Before engaging with this case, students should have a foundational understanding of several key frameworks and concepts for analyzing the situation. These include governance and risk management models, fraud prevention techniques, information security practices, and the challenges associated with unauthorized technology use. Table 1 outlines the essential prerequisites that students should be familiar with to effectively navigate the case and apply critical thinking to the analysis. Recommended readings, videos, and handouts have been provided, but textbooks from major publishers may also cover these prerequisite topics.

Table 1

Recommended Prerequisite Topics

Topic	Brief description	Recommended reading	Recommended video	Recommended handout
COSO framework	The COSO framework guides organizations in implementing controls to prevent, detect, and manage fraud in external financial reporting.	https://auditboard.com/blog/coso-framework-fundamentals/	https://share.vidyard.com/watch/MPiwSXEo4AAgK33xETfXB6?	https://www.coso.org/_files/ugd/3059fc_77d5d0f3d569439990b170bd3b909d7e.pdf
COBIT framework	The COBIT framework offers comprehensive guidelines for effective IT governance and management.	https://www.auditboard.com/blog/cobit/	https://youtu.be/KJLAJSZbfIM	COBIT | Control Objectives for Information Technologies | ISACA
Fraud triangle / professional skepticism	The fraud triangle was developed by Dr. Donald Cressey, a criminologist whose research on embezzlers produced the term "trust violators" (Marquart & Thompson, 2024). Professional skepticism enhances fraud detection.	https://corporatefinanceinstitute.com/resources/accounting/fraud-triangle/	https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud	https://blog.lowersrisk.com/wp-content/uploads/2020/11/lrg-fraud-triangle.pdf
Information security policy	An Information Security Policy (ISP) is a formal document that outlines an organization's guidelines and measures for protecting the confidentiality, integrity, and availability of its information assets.	https://blog.netwrix.com/information-security-policy	https://www.rsaconference.com/library/presentation/usa/2019/back-to-the-basics-how-to-create-effective-information-security-policies	https://www.sans.org/information-security-policy/?category=general
Shadow IT	Shadow IT refers to any software, hardware, or IT resource used within an organization's network without the IT department's approval, awareness, or supervision.	https://www.auditboard.com/blog/2022-security-risk-trends-report-key-takeaways/	https://www.ibm.com/topics/shadow-it	https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoYyEAK

Implementation Guidance

To implement the role-play, we separate the case into two sections including 1) Initial Activities and 2) Running the Role-Play.

Initial Activities

For smooth facilitation, the initial activities should be completed before the role-play begins. These activities include reviewing the prerequisite topics (Table 1), preparing and printing the necessary tangible role-play materials (Appendices A and B), and scheduling how the role-play will fit into the class timeframes (e.g., one three-hour class versus two 75-minute classes) (Table 2).

1. Prerequisites: Reviewing or teaching the recommended prerequisite topics in Table 1 before the role-play ensures that all students understand the referenced AIS topics equally. The topics have been listed with a summary and links to additional resources. Additionally, course-specific textbook materials might cover the topics in detail.
2. Materials: Preparing the materials by printing the case study, backstories, name badges, and table tents before running the role-play is essential to guarantee a seamless role-play. Copies of the scenario, name tags, double-sided name plates, and individual character backstories are needed for every group of students. Materials can be printed or distributed digitally, but name tags and nameplates must be physical.
    - A PowerPoint (based on the Teaching Notes) with directions for conducting the role-play, guiding questions, and critical details is a helpful way to present a visual for both the instructor and the student. It can be adapted for an adjusted timetable (Table 2) and modified deliverables.
3. Timetable: The role-play can be conducted in a single class (~3 hours) or divided into multiple sessions using the timetable (Table 2). The timetable lists minimum durations for each part of the role-play, allowing instructors to extend time as needed for each step.
    - Additionally, some activities (e.g., forming groups and reviewing prerequisite topics) may be completed online or assigned before class time begins. Strategic stopping points are included in the timetable as recommendations to allow for the duration of the class or as an opportunity for students to complete work outside class without disrupting the role-play's momentum.

Table 2

Role-Play Timetable

Activity	Class, group, individual	Duration (min)
Form groups	Group	0–5
Read role-play scenario (Appendix A, Scenario Handout 1)	Class	10–15
Create deliverable 1	Group	25–30
Stop point to accommodate 50-minute class.		
Read character backstories (Appendix B)	Individual	5–10
Create deliverable 2	Group	25–30
Stop point to accommodate 50-minute class.		
Role-play 10:00 a.m. meeting (Appendix A, Scenario Handout 2)	Group	15–20
Create deliverable 3	Group	5–10
Stop point to accommodate 50-minute class.		
Hold post-mortem	Class	10–15
Create deliverable 4	Group	5–10
Class discussion	Class	10–15
Stop point to accommodate 50-minute class.		
Create deliverable 5	Group	Instructor Defined
Presentations	Group	Instructor Defined

Once the initial activities are complete, the role-play itself is ready to begin. The steps to run the role-play are outlined in a recommended sequence to ensure smooth progression and maintain engagement.

Running the Role-Play

The role-play is written in a framework like a "whodunit mystery," where each participant only knows their part of the story until everyone begins to share and collect details from the other players. Slowly, the entire story comes together. Because students might not be familiar with "whodunit" role-plays, introducing the concept beforehand can

help set expectations. Introducing the idea of a "whodunit mystery" could involve students sharing examples of movies where viewers try to solve a complex mystery.

It is also important to introduce students to the process of role-playing. Role-play is an active learning strategy that simulates real-world situations, allowing students to immerse themselves fully in their roles and treat the experience as a simulation of real-life organizational dynamics. Students should approach the activity as if they are putting on a school play, fully embracing their character's role and interacting naturally with others to bring the scenario to life. This immersive approach encourages critical thinking and real-world decision-making, enhancing students' grasp and retention of key concepts.

Providing the rubric for role-play (Table 3) helps students focus on the necessary deliverables, avoid distractions, and align their efforts with the primary learning goals. Staying in character is essential for maximizing this immersive experience. Breaking character disrupts the flow, causes confusion, and may lead to missed opportunities for meaningful insights. Active participation ensures students uncover key details rather than relying on passive observation.

1. Form Groups:
    - Each group will perform the role-play. The groups should consist of six students corresponding to each of the six roles in the role-play. The groups should be organized in the classroom so that there is space between the groups to foster authentic discussion within each group. The case allows the selection of two choices in names for each character (e.g., Miranda or Matt, Sumi or Sam) to allow customization by the group.
        - If there are insufficient students for six-person groups, Brad and his related deliverables can be removed from the role-play.
        - Alternatively, several students can act out the role-play in front of the class while others observe. This approach provides less hands-on experience but offers a creative way to explore the material.
2. Introduce Scenario:
    - The instructor reads the scenario (Appendix A) to the class, stopping before the section titled 10:00 a.m. Meeting: The Confrontation. If possible, the instructor should distribute printed copies of the scenario to each group, ensuring students see only the approved sections. The backstories and later sections of the scenario should remain hidden until the appropriate time. To make sure students have a good understanding of the scenario and the concepts and frameworks (i.e., COBIT and COSO frameworks, fraud triangle, information security policies, ghost employees, and shadow IT), students have these tasks:
        - Deliverable 1 Organization Chart (Optional): Groups should create an organizational chart based on each involved company's scenario (Table 3), illustrating their interactions. While creating the organizational chart is an optional deliverable and not directly aligned with the learning objectives, it serves two valuable purposes.
            1. Encourage collaboration.
            2. Provide a visual reference during the role-play, clarifying roles and responsibilities.
        - Deliverable 1 Questions: To ensure understanding, students should answer the questions found in Table 3.
3. Distribute Backstories
    - After students complete Deliverable 1, the instructor distributes backstories (Appendix B), table tents, and name tags. Delaying this step ensures students work through the scenario systematically.
    - Students must wear name tags displaying their character name and role to reduce confusion, reinforce hierarchy, and simplify discussions with the instructor. To avoid confusion, group members must be addressed by their character's name.
    - Each group member will receive a character backstory (Appendix B) that only they will see, as each character's story contains unique information. This will ensure the "whole story" emerges as students decide what to share and when. It is important that each backstory be on its own page so that students only receive information about their role. Students should take time to read their backstory and refrain from talking amongst their group.
        - Deliverable 2 Timeline (Optional): Groups should be given time to create a timeline of events (Table 3). Students must only reveal character names and the guidepost times: ERP upgrade begins, ERP upgrade continues, ERP upgrade freezes, ERP upgrade is fixed and completed, upgrade process meeting, keeping backstory details confidential. While optional, the timeline encourages group collaboration and provides a visual reference during the role-play.
4. Continue Scenario: When ready, the faculty can pass out the remainder of the 10:00 a.m. Meeting: The Confrontation section and give the groups time to play out what will happen. Between the scenario and the

individual backstories (Appendix B), students should be able to piece together what the day will look like. At this stage of the role-play, students will encounter the most ambiguity, as the scenario will unfold based on how each participant chooses to play their role.

- The instructor should encourage students to immerse themselves fully in their roles and interact as their assigned characters, treating the experience like an improvisational play. Each student should use their character's name, engage naturally with others, and let interactions develop as they might in real life.
- There is no specific script or exact way to play the role, so the interactions develop naturally. Students can share details from their character's backstory at their discretion, but they should avoid revealing too much at once.
    - Deliverable 3 Questions: After the role-play of the meeting, students will create a document to record their answers to the questions outlined in Table 3.

5. Hold Post-Mortem: The students must hold a post-mortem to reflect on the entire scenario and how the role-play unfolded.
    - Deliverable 4: A collaborative document will be created by all group members to answer the questions outlined in Table 3.
6. Class Discussion (Optional): This optional activity allows students to reflect on the role-play. Additionally, it can be a time when the instructor can act as a skeptic, taking on viewpoints that students might not have considered. For example, if most students believe that someone is guilty, it can be helpful to challenge them with reasons why the person may not be guilty. Sample alternative viewpoints are listed in the Teaching Notes. If time is not available for an in-class discussion, it can also occur online through a discussion board or be omitted altogether.
7. Group Presentation (Optional): After completing the role-play and Deliverables 1–4, the instructor may require students to participate in an optional group presentation.
    - Deliverable 5: This presentation can analyze the decisions made during the role-play, drawing on the ISP protocol, COSO and COBIT frameworks, and the fraud triangle. The presentation encourages further discussions and reinforces learning objectives. Alternative concluding deliverables could include short answer questions, test questions, or discussion board activities.

Deliverables

Table 3 outlines the role-play deliverables, which can be modified to align with various levels, goals, or course requirements.

Table 3
Role-Play Deliverables

#	Deliverable(s)
Deliverable 1	An organizational chart (optional) for each company involved, showing how the two companies will interact. A document with an answer to these questions: • Identify and list relevant issues related to the COBIT framework, COSO framework, Information Security Policy (ISP), and potential fraud. • Categorize each issue within the respective framework and briefly explain.
Deliverable 2	A timeline (optional) of activities can be updated as the role-play continues. Items to be on the timeline (identify who is involved and the time it takes place): • ERP upgrade begins • ERP upgrade continues • ERP upgrade freezes • ERP upgrade is fixed and completed
Deliverable 3	A document answering the following questions: 1. COSO framework • Identify multiple possible violations and weaknesses. • Identify areas of control that have vulnerabilities. • What could an IT audit function do to help Blue House? 2. COBIT framework • Identify multiple possible violations and weaknesses. • Identify areas of control that have vulnerabilities. • What could an IT audit function do to help Blue House? 3. Using the fraud triangle and your professional skepticism/judgment: • Place each character under scrutiny and identify how each character may or may not be prone to commit fraud (assessing misappropriations or financial misstatement misconduct). • Include any other concerns for improvement for Blue House. 4. Using what has been mentioned and contained in the company ISP, were there any violations? • Identify multiple possible violations and weaknesses. • If there were ISP violations, were they malicious or non-malicious?
Deliverable 4	A document answering the following questions: • Does the Lakers ERP Senior Consultant get fired by the Lakers CTO & Managing Partner, and if so, for what reasons? • Should the Lakers ERP Senior Consultant face charges, and if so, what? • Is the CTO & Managing Partner accountable for any issues with the upgrade or hold responsibility in the upgrade process? • What are some considerations regarding the relationship between Blue House and Lakers Consulting? • What potential consequences could the CTO face if held accountable for his/her actions? • What best practices should Blue House implement for password management to strengthen their security posture? • Is the Senior Accountant accountable for any issues with the upgrade, or does he/she hold responsibility in the upgrade process? • Does the Senior Accountant get fired by the CEO, and if so, for what reasons?
Deliverable 5	A group presentation (optional) including: • Summary of the role-play scenario. • Deliverables 1–4 in summary. • Explanations of how things should have been done differently. • Conclusion or overall findings.

Efficacy

The role-play was implemented across four AIS courses: three undergraduate courses, each with approximately 36 students, and one graduate course with around 20 students. The undergraduate courses primarily consisted of third- and fourth-year students, many of whom had internship experience in audit or tax. Similarly, the graduate students were mainly fifth-year seniors working to complete their 150-hour requirement, with comparable backgrounds in audit or tax internships.

To enhance the efficacy and realism of the role-play, the authors collaborated with an additional accounting instructor who reviewed the case and implemented it in their own class. Based on this feedback, revisions were made to refine the role-play, ensuring greater authenticity and a stronger focus on specific accounting challenges within organizations. These enhancements improved the alignment of the activity with real-world accounting practices, providing students with a more meaningful and immersive experiential learning opportunity.

Following the role-play, students responded to three prompts, sharing their impressions of the activity. This verbal feedback was then summarized for analysis, revealing no significant differences between the undergraduate and graduate groups. Despite natural variations in experience and course level, undergraduate and graduate students expressed similar perspectives.

Table 4
Student Feedback

Prompt	Student Feedback
The role-play we played in class helped me understand . . .	Overall, the feedback on the role-play expressed that students gained a deeper understanding of the course objectives, specifically the COSO and COBIT frameworks, solid information security policy (ISP) practices, and the fraud triangle. Engaging in character-driven scenarios allowed students to connect these concepts to real-world situations, making the frameworks and security principles more accessible and relevant to their learning. Many students appreciated how the activity clarified these structures, enhancing their ability to apply them thoughtfully in practical contexts. Specific comments included: • "During this role-play, I found it difficult to act as the character because I disagreed with their actions. But it gave me insight into decisions and motives I had never thought of before." • "One major aspect of this class I have noticed so far is that everyone thinks differently."
The role-play approach is enjoyable . . .	The feedback highlighted the effectiveness of applying AIS concepts to realistic scenarios, allowing students to engage with real-world dilemmas from varied perspectives. Students appreciated the opportunity to practice handling issues they may encounter in their careers, finding the experience engaging and insightful. Specific comments included: • "I have enjoyed the role-play, and it does a great job applying our knowledge of AIS topics to real-world situations. I also like that they have us view dilemmas from different points of view than we would normally take." • "I love the role-play that we did in class. It gives everyone a chance to be involved in a 'real-life' situation that we all might have to deal with at some point."
The role-play approach enhanced my learning . . .	Feedback on the role-play indicated that students found this method encouraged critical thinking and facilitated the application of lecture material to practical situations. Overall, the experience was viewed as more valuable than traditional memorization, promoting deeper engagement with the subject matter. Specific comments included: • "I think the thing about the role-plays that makes them so successful is the fact that they are real situations. It is one thing to be put in a hypothetical scenario. . . . [T]his situation actually happened, and it makes me actually think about what I would actually do in the real world." • "This has helped me the most in taking the material out of the lecture and applying it to real situations." • "The requirement to put ourselves directly in the role-play that was presented to us will, in my mind, benefit us much more than some spreadsheet or formula we had to memorize."

Conclusion

Students entering accounting roles will be expected to work in technology-driven environments requiring information security and data management oversight. Role-play exercises represent a promising pedagogical method for facilitating a deeper and more critical understanding of decision-making related to AIS and evolving cybersecurity issues. This paper presents an experience report of a role-play exercise conducted in a medium-sized, four-year public university in the United States. Results suggest increased student engagement in applying concepts from the COSO and COBIT frameworks and applying professional skepticism and the fraud triangle to information security policy violations that may lead to catastrophic consequences for an organization. The role-play encourages students to express multiple points of view regarding cybersecurity, internal controls, and fraudulent financial activities. The material and suggestions provided in this report may also aid other faculty in facilitating a business role-play for students to collaborate and communicate professionally.

References

Association of Certified Fraud Examiners (ACFE). (n.d.). *Fraud 101: What is fraud?* https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

AuditBoard. (n.d.). *COSO framework explained* [Video]. Vidyard. https://share.vidyard.com/watch/MPiwSXEo4AAgK33xETfXB6

AuditBoard. (2022). *2022 security risk trends report: Key takeaways*. https://www.auditboard.com/blog/2022-security-risk-trends-report-key-takeaways/

AuditBoard. (2024). *COBIT: IT governance and management explained*. https://www.auditboard.com/blog/cobit/

Bee, S., Parra, F., & Bailey, A. (2021). Using COSO to mitigate service learning project risk. *AIS Educator Journal*, *16*(1), 40–59. https://doi.org/10.3194/1935-8156-16.1.40

Boyce, G., Greer, S., Blair, B., & Davids, C. (2011). Expanding the horizons of accounting education: Incorporating social and critical perspectives. *Accounting Education*, *21*(1), 47–74. https://doi.org/10.1080/09639284.2011.586771

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. *Decision Sciences*, *49*(6), 1187–1228. https://doi.org/10.1111/deci.12304

COSO. (n.d.). *COSO internal control—Integrated framework principles* [Infographic]. https://www.coso.org/_files/ugd/3059fc_77d5d0f3d569439990b170bd3b909d7e.pdf

Corporate Finance Institute. (n.d.). *Fraud triangle*. https://corporatefinanceinstitute.com/resources/accounting/fraud-triangle/

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

IBM. (2022, August 4). *What is shadow IT?* https://www.ibm.com/think/topics/shadow-it

ISACA. (2019, November 7). *Introducing COBIT 2019* [Video]. YouTube. https://www.youtube.com/watch?v=KJLAJSZbfIM

ISACA. (n.d.). COBIT | Control Objectives for Information Technologies.

Kesler, C. (2019, March 5). *Back to the basics: How to create effective information security policies* [Conference session]. RSA Conference 2019, San Francisco, CA, United States. https://www.rsaconference.com/library/presentation/usa/2019/back-to-the-basics-how-to-create-effective-information-security-policies

Kouchaki, M., & Desai, S. D. (2015). Anxious, threatened, and also unethical: How anxiety makes individuals feel threatened and commit unethical acts. *Journal of Applied Psychology*, *100*(2), 360–375. https://doi.org/10.1037/a0037796

Lehmann, C. M., & Hao, J. (2020). Understanding the COSO 2013 framework: Four short cases for use in AIS and auditing courses. *AIS Educator Journal*, *15*(1), 1–24. https://doi.org/10.3194/1935-8156-15.1.1

Leland, A. (2024, June 20). *Fundamentals of the COSO framework: Building blocks for integrated internal controls.* AuditBoard. https://auditboard.com/blog/coso-framework-fundamentals/

Lowers Risk Group. (2020). *The fraud triangle* [Infographic]. https://blog.lowersrisk.com/wp-content/uploads/2020/11/lrg-fraud-triangle.pdf

Marquart, J. W., & Thompson, R. A. (2024). Exploring relation fraud, murder, and the fraud triangle. *Journal of Economic Criminology*, *4*, 1–6. https://doi.org/10.1016/j.jeconc.2024.100061

Martins, A., & Elofe, J. (2002). Information security culture. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan. (Eds.), *Security in the information society* (pp. 203–214). Springer. https://doi.org/10.1007/978-0-387-35586-3_16

Posey, C., & Folger, R. (2020). An exploratory examination of organizational insiders' descriptive and normative perceptions of cyber-relevant rights and responsibilities. *Computers & Security*, *99*, 102038. https://doi.org/10.1016/j.cose.2020.102038

Powell, L., Lambert, D., McGuigan, N., Prasad, A., & Lin, J. (2020). Fostering creativity in audit through co-created role-play. *Accounting Education*, *29*(6), 605–639. https://doi.org/10.1080/09639284.2020.1838929

SANS Institute. (n.d.). *Security policy templates*. https://www.sans.org/information-security-policy/?category=general

Selart, M., & Johansen, S. T. (2011). Ethical decision making in organizations: The role of leadership stress. *Journal of Business Ethics*, *99*(2), 129–143. https://doi.org/10.1007/s10551-010-0649-0

Sotnikov, I. (2023, December 20). Information security policy: Must-have elements and tips. *Netwrix Community*. https://blog.netwrix.com/information-security-policy/

We would like to acknowledge the assistance of AI-based tools, such as OpenAI's ChatGPT, in providing feedback on the structure, formatting, and clarity of this paper. These suggestions were instrumental in refining the overall readability.

Appendix A

Scenario Handout 1

Summary

The role-play "The Sunday Standstill" is a unique learning experience structured as an interactive activity based on a real-life scenario. It immerses students in the intricacies of internal controls related to the ISP protocol, COSO and COBIT frameworks, and fraud triangle. The scenario details are initially vague, but as the role-play unfolds, additional details emerge, challenging students to apply their knowledge and problem-solving skills. Like a "whodunit" mystery, the exercise promotes collaboration and critical thinking.

Characters

Lakers Consulting Company

- Miranda/Matt* – Chief Technology Officer (CTO) & Managing Partner
- Greg/Gracie* – ERP Senior Consultant

Client Company: Blue House

- Brad/Brittany* – Chief Executive Officer (CEO)
- Jessie/John* – Chief Financial Officer (CFO)
- Sumi/Sam* – Chief Technology Officer (CTO)
- Andrew/Angelica* – Senior Accountant

*Two names per role have been provided, allowing for adaptation and student preference.

Background

Blue House has hired Lakers Consulting to complete an urgent IT systems upgrade. Blue House currently uses two separate information systems: 1) an accounting system (AIS) and 2) a manufacturing system (MRP).

The AIS system does not automatically integrate with the MRP system. Therefore, it cannot provide real-time cost tracking for manufacturing activities, such as automatically capturing employees' work hours. As a result, separate ledgers are required for manufacturing (employee hours worked) and operational costs (pay rate).

Currently, Blue House tracks employee hours manually. Andrew, Blue House's senior accountant, collects employees' work hours and enters them into the AIS system. This is usually completed on a Saturday so the entire week can be tabulated in one sitting. Andrew comes into the office for two hours every Saturday afternoon, completes the tabulations, and then submits the final figures. There are no cross-check protocols in place.

Upgrade Preparation

In preparation for the upgrade, Sumi (Blue House's CTO) has analyzed and documented the current process and checked the accuracy of recent payroll submissions in preparation for the upgrade. Based on the investigation, a few names appeared on the old payroll records but had no corresponding HR or timekeeping log entries. While it could be a data mapping issue, Sumi made a mental note to follow up with Andrew during the week. Sumi is concerned about this vulnerability in their IT general controls and the company's broader financial health and wonders if they will pass their annual audit.

Sumi's Concerns

Sumi is aware that Blue House has inadequate information security and has noted two concerns. First, the AIS and MRP systems are so outdated that security patches are no longer available, leaving the systems vulnerable to cyberattacks. Second, due to the age of the system and lack of ability to change anything now that it is no longer being supported, the team has been sharing several standard login and password combinations to log into the systems, limiting the system's ability to track who and when someone completes transactions. These login credentials are pinned to a bulletin board in a shared office to which all team members have access.

Blue House developed its internal IT controls using the COSO and COBIT frameworks. Sumi applied the COSO framework to enhance enterprise risk management and internal control principles, promoting a risk-aware culture. Sumi then used the COBIT framework for detailed guidance on IT governance and management, focusing on information security, compliance, and IT operations. Earlier this year, Blue House experienced several cyberattacks focused on credential theft, and Sumi used COBIT guidelines to write a new section in their information security policy (ISP) for credentials. The new policy requires employees to have their own credentials, store passwords securely, and not share passwords without authorization. Consultants are provided with temporary credentials and passwords to have limited access to controlled data.

Even with these concerns identified by Sumi, Blue House would have liked to continue with its current systems. However, this is not an option, given that their current software provider has decided to discontinue the software

within a year, necessitating immediate action.

Upgrade Details

The upgrade plan provided by Lakers Consulting involves consolidating the two separate systems (AIS and MRP) into a robust Enterprise Resource Planning (ERP) system. This will benefit Blue House in several ways.

First, it would enable real-time data integration between the AIS and MRP systems, allowing for accurate and timely cost tracking related to manufacturing activities. This includes automatically capturing employees' work hours and applying pay rates, which streamlines labor cost tracking.

Next, consolidating the systems eliminates the need for separate ledgers for manufacturing and operational costs, providing a more precise and cohesive financial picture.

Third, the upgrade also addresses the current security issues with the most current embedded systems, which protect against cyberattacks and proactively apply security patches to remain current. The upgrade also aligns with the newly created ISP protocols, giving each employee their own login credentials and allowing the system to track who is in the system and what transactions they are completing.

Finally, by migrating to an ERP system, Blue House avoids the impending software sunset of the current accounting system, ensuring continuity and long-term support for its financial software needs.

The Upgrade Team: Greg, Sumi, and Andrew

A small team consisting of Blue House and Lakers Consulting employees has been formed to oversee the upgrade.

Project Co-owners:

- Greg (Lakers ERP Senior Consultant)
- Sumi (Blue House CTO)

Upgrade Leader:

- Greg is reporting to Miranda (Lakers CTO and Managing Partner).

Accounting team member:

- Andrew, Blue House's senior accountant, is on the team because Sumi manages the maintenance of the accounting system and collaborates closely with Andrew.
- Both Sumi and Andrew report to Jessie (Blue House's CFO) for the duration of the upgrade.

Upgrade Timing

Traditionally, ERP upgrades are scheduled to take place over a weekend, so they are complete and ready by Monday morning, at the start of the manufacturing shift. This avoids the need to stop manufacturing during the regular work week. The Blue House upgrade is scheduled to begin on Friday at 5:00 p.m.

The upgrade team (Greg, Sumi, and Andrew) will be on-site to shut down the current AIS and MRP systems. They will remain on-site until the upgrade is complete, which is planned for Sunday evening.

Commencing the Upgrade

All team members meet on-site on Friday at 5:00 p.m., as planned. Greg, Sumi, and Andrew work through the upgrade plan, taking data from the two existing systems and saving it in the cloud. The data categorization and validation is completed, and the data is prepared to be placed into the new ERP system in the proper data tables.

Together, the team works through the night Friday. Greg is taking the lead, Sumi is assisting, and Andrew is answering questions relating to accounting, as required. They sleep only a few hours on Friday evening and Saturday evening, working steadily and making progress. On Sunday morning, however, things go wrong.

At 10:00 a.m., Greg is surprised that the data transfer has stopped, and everything is frozen. The upgrade is only partially complete and cannot be reversed back, and because the upgrade is not entirely complete, both the old systems and the new ERP system are locked and unavailable.

Greg believes an internal computer process is holding up the upgrade, but no one can determine which process it is. The team contacts technical support for the ERP system and is told that the on-site support team will be sent immediately but won't arrive due to flight scheduling until Monday morning. The team has no way to make any more progress on the upgrade, so by 1:00 p.m., Greg and Sumi decide that everyone should go home.

Scenario Handout 2

10:00 a.m. Meeting: The Confrontation

Miranda is in the conference room, setting up breakfast, when Sumi, Andrew and Jessie arrive. Miranda is puzzled by the atmosphere in the room; Sumi and Andrew appear visibly angry while Jessie appears confused. Greg arrives last and takes a seat.

Just as the meeting is about to begin, Brad walks by and glances into the room. Brad pauses, looks around the room, and then says, "This looks like an important meeting, so I am going to join if you don't mind" then takes a seat at the table.

Jessie speaks first, asking why the manufacturing floor is operating given that the upgrade stalled on Sunday and was not going to be fixed until Monday. Sumi begins speaking and explains how the entire team worked on the ERP upgrade from Friday evening to Sunday morning. On Sunday, the upgrade stalled due to a system process, and the team did not know the actual problem. The team tried contacting technical help but found it was unavailable until Monday morning. For this reason, Sumi, Andrew and Greg all left at 1:00 p.m. on Sunday and had all agreed to stop work and reconvene on Monday morning.

Sumi explains to the room that Sumi and Andrew received some vague text messages from Greg later Sunday evening, and Sumi had replied with "What's up?" only to receive Greg's reply at about 1:00 a.m. that said, "Never mind".

Sumi and Andrew came to work this morning, prepared for everything to be still frozen but instead found the upgrade complete. Sumi and Andrew reviewed the system and found that Sumi's credentials were used on Sunday to access the system. Given that Sumi had not logged in, the only logical explanation was that Greg had used Sumi's credentials without permission, gaining access to the highest level of data in the systems. As Sumi finishes speaking, Brad turns to the consultants and asks, "Is this true?"

Miranda, Lakers Consulting CTO and Managing Partner, begins speaking. Miranda explains Lakers' commitment to excellence, clear communication, and high expectations. Miranda explains that these characteristics are expected from all Laker's employees and that deviations are treated seriously. Miranda then turns to Greg and poses the question, "Greg, is what Sumi said accurate?"

Greg's Response

Greg begins offering an explanation of what occurred on Sunday, and it is very different from that of Sumi and Andrew. Greg points out that the actions taken were needed to get the job done. Greg explains that the actions taken theoretically saved Blue House thousands of dollars that would have been incurred if the production line was down during the work week. For this reason, bypassing established protocols for accessing credentials was justifiable. Greg also points out that Sumi has the list of credentials printed on a bulletin board in plain sight, and the list was even shared on a few occasions.

Finally, Greg adds that Andrew had mentioned several times that Sumi has problems paying attention to details and is exceptionally nervous around high-level technology. Therefore, Greg believed that Sumi would have agreed to whatever was necessary to get the ERP system upgrade completed by the deadline. Greg's final points are threefold: Brad should be thankful for Lakers finding the real reason for the significant error in the payroll system, ghost employees have been fraudulently entered into the system, and an investigation is needed urgently.

Brad and Jessie are both dumbfounded by the information disclosed. A number of important questions are being considered:

- Who is to be believed?
- Who, ultimately, is responsible for the actions of the Blue House staff?
- How did Jessie allow this project to go off the rails like this?
- How did the payroll's significant error not get identified sooner?
- How fast can the legal department review these circumstances for fraud, ISP violations, and any COSO or COBIT violations?
- Is this project a failure or a success?
- How did Sumi allow this to happen? With Sumi as CTO, are the controls in place being followed or even effective? Is Sumi qualified for a high-level position like CTO?
- Why was Greg allowed to lead this project when there have already been issues in previous projects?
- Should it be considered that Greg saved Blue House thousands of dollars, or more, by fixing the stalled upgrade?

Appendix B

Character Backstories

Greg's Backstory

Greg (Lakers Consulting ERP Senior Consultant)

Greg has been with Lakers Consulting for seven years and, during this time, has been promoted to the position of ERP Senior Consultant. Greg is very bright and hard-working but has a strong personality that can come across as brash and dismissive. Greg works very fast and never misses a deadline but has been known to sacrifice accuracy along the way. Most of Greg's colleagues now do not trust the work put out by Greg unless it has been reviewed or checked by another member of the team.

Because of this tendency for carelessness, Lakers' managing partner, Miranda, has recently put Greg on a Performance Improvement Plan (PIP). The PIP calls for Greg to improve in several key areas or face dismissal. When the PIP was introduced to Greg, Greg was secretly furious and felt it was an overreaction. The PIP has made Greg even more committed to showing everyone they underestimated Greg's skills and potential.

The Fix

After a few hours of sleep at home, Greg suddenly realizes what is preventing the system upgrade from completing. Greg recalled a similar stall from a previous ERP project in which a locked accounting ledger halted progress during the data migration phase. Upon reviewing the error logs and observing the system's behavior, Greg suspected the current issue was identical: an internal ledger process prevented the upgrade script from completing its run. Recognizing that resolving the problem required administrative access typically reserved for the CTO, he deduced that using those credentials could override the blockage and allow the installation to resume. It is 9:00 p.m. on Sunday, and Greg sends out an email to the upgrade team. When no email replies come through, Greg also sends an urgent group chat message as well as phoning each of the team members directly. However, the messages remain unread, and all calls go straight to voicemail.

Greg sits at home anxiously waiting; hours pass with no replies. After two hours of silence, Greg worries that further delays could jeopardize the project's success. With the system locked and the deadline looming, Greg feels compelled to act independently. As the ERP Senior Consultant, Greg recognizes a heightened responsibility to resolve the issue, believing that swift, decisive action is essential to demonstrate leadership in this crisis.

Greg believes that unlocking the upgrade requires access to critical files and changes to an accounting ledger process in the ERP system. With the high-level ISP access control at Blue House, consultants are provided with temporary credentials that limit what can be accessed. Therefore, Greg cannot access the process without Sumi's credentials being used. Greg makes several more attempts to contact the upgrade team, specifically trying to reach Sumi so Sumi's credentials can be used to access the process in the system. After a few more hours without success, Greg has had enough. Greg's previous experiences with Blue House have been strained, and any further conflict could harm Lakers Consulting's credibility with the client. Miranda would not tolerate any loss of trust, and firmly believes that further client friction could lead to dismissal. Greg decides to act independently; Greg's job needs to be protected as well as the client relationship and project continuity.

Earlier in the project, Greg noticed that Sumi kept usernames and passwords on a bulletin board behind the monitor in Sumi's office. Sumi had mentioned that since so many employees shared credentials, it was easy to just keep a physical list of them for reference. Sumi even asked Greg to reference this list several times during the upgrade, so much so that Greg had taken a photo of the list for easy reference, without Sumi knowing.

Using Sumi's credentials, Greg logs into the system, accessing all of the required system processes. Within 10 minutes, Greg makes the required changes, and the upgrade process starts to run again. By 1:00 a.m., Greg completes the upgrade.

Just as the upgrade finishes, Greg receives a response to the group text, asking "What's up?" to which Greg replies, "Never mind." Greg is exhausted, wants to sleep, and feels no need to explain the night's events. It will take far too much energy to rationalize to the team why bypassing established protocols for accessing credentials is justifiable and why it was necessary to prioritize immediate resolution over compliance.

Greg sends Miranda (Lakers' CTO and Managing Partner) an email at 1:00 a.m. stating that the upgrade is complete, and the factory will start operation on time Monday morning.

Monday

It is Monday morning, and Greg is up early preparing to head into Blue House for meetings. Greg takes a moment to reflect on the potential positive career effects of this upgrade project. Greg is up for a promotion and a significant bonus, both of which hinge on successfully completing the upgrade at Blue House. Throughout the project, Greg has

been keenly aware that any issues with the project or loss of client trust could have jeopardized these prospects. Greg is content with the decisions made to complete the update.

Additionally, Greg assumes Sumi, Andrew, Jessie, and Miranda will be thrilled to hear that Greg worked through the night to make the project successful. Greg's efforts theoretically saved Blue House thousands of dollars they would have incurred if the production line was down during the work week.

Miranda's Backstory

Miranda (Lakers Consulting Chief Technology Officer and Managing Partner)

Miranda has been the Managing Partner at Lakers Consulting for over a decade, during which time a strong working relationship with Blue House has been cultivated. Miranda's relationships with key Blue House personnel (namely Sumi and Andrew) have been largely positive, mainly because Sumi appreciates the expertise Lakers Consulting brings to the table for ERP upgrades and maintenance. However, Miranda finds Andrew to be rigid and uncooperative when accessing accounting data, which can complicate interactions.

Miranda's leadership style emphasizes excellence, clear communication, and high expectations. It fosters growth and accountability while directly influencing team members' career progression and the organization's success.

Miranda has been instrumental in mentoring Greg to become a Senior Consultant, but lingering concerns remain. Miranda knows that Greg has a history of avoiding necessary help and dismissing the importance of having work checked by others, which has raised red flags.

Because of these recurring concerns, Miranda placed Greg on a Performance Improvement Plan (PIP), effectively Greg's last chance. Miranda has clearly outlined to Greg the expectations in the PIP: Greg must complete the project while maintaining the firm's high standards in terms of work quality and protocols. Failing to meet these expectations will result in Greg's termination, while demonstrating success will lead to a promotion and a substantial bonus. Miranda hopes this will motivate Greg to rise to the challenge. Needless to say, Miranda was delighted and relieved to receive Greg's 1:00 a.m. email confirming that the update was successfully completed.

Monday's Agenda

Miranda has two meetings scheduled at Blue House for Monday: an 8:00 a.m. meeting with Greg to discuss the upgrade project details, and a 10:00 a.m. onsite meeting with Sumi, Andrew, and Blue House's CFO, Jessie. Miranda is a bit old-fashioned and feels that being present in the office the morning after an upgrade and bringing in a celebratory breakfast goes a long way in maintaining the firm's reputation and securing future consulting opportunities. At the 10:00 a.m. meeting, Miranda plans to discuss the successful upgrade project and the strong ongoing relationship with Blue House and how this successful upgrade can build Jessie's trust in Lakers Consulting. Also, Miranda is aware that Greg appears to have successfully met the criteria on the PIP, therefore securing a promotion and raise.

Meeting #1: 8:00 a.m.

The first meeting between Miranda and Greg goes as planned. Greg explains that Greg's project leadership that was demonstrated was critical to the successful upgrade. Greg reminds Miranda that the actions taken during the project were all the criteria listed in the PIP, and therefore the topic of promotion and bonus should be discussed.

Sumi's Backstory

Sumi (Blue House Chief Technology Officer)

Sumi's career at Blue House started over 10 years ago in the accounting department, managing overdue accounts receivables before moving to the technology help desk. These diverse experiences gave Sumi a unique understanding of the interactions between accounting and manufacturing systems. Sumi does not have a formal degree in accounting or information technology but has always been positive and a quick learner. Therefore, Sumi has been promoted several times. The most recent promotion to CTO was a big surprise to everyone at Blue House, including Sumi! As CTO, Sumi collaborates with Andrew, the Senior Accountant, and reports to Jessie, the CFO.

Sumi and Andrew have previously hired Lakers Consulting to make some small ERP system changes, such as updating employee addresses or adding new part numbers to their master data. Sumi recognizes the importance of bringing in outside experts, especially given that Sumi has yet to study IT at the university level formally. Sumi believes hiring external consultants improves success rates, and Blue House enjoys collaborating with Miranda.

However, reservations about Greg, Lakers' ERP Senior Consultant, exist. These reservations are based on some past negative experiences that left Sumi feeling somewhat uneasy. But given their expertise in ERP systems and IT security, Sumi was in support of hiring Lakers Consulting to handle this ERP upgrade.

Discovering the Stall

At 7:00 a.m., Monday morning, Sumi arrives at Blue House and is shocked to find the factory running smoothly. Perplexed, Sumi completes a cursory review of the systems and sees the new system up and running. Sumi catches Andrew as soon as Andrew walks in the door explaining that somehow, miraculously, the new system is running. Andrew, who is very rigid about accounting data, is naturally suspicious.

Sitting down in Sumi's office, Andrew asks Sumi to log in to the system to figure out whose credentials had been used to access the system within the last 24 hours. The list appears accurate until Andrew notices that Sumi's credentials had been used at about 12:30 a.m. Sumi knows this is impossible, but why is Sumi's name on the list? The only thing that Sumi and Andrew can assume is that Sumi's credentials were used by Greg. Sumi is furious and, at the time, indignant because past interactions with Greg have been negative. Sumi regrets giving Greg too many chances, even after Greg showed a tendency to be hasty with work and cut corners in order to make deadlines. Sumi plans to present the evidence in the 10:00 a.m. meeting with Miranda, hoping for Greg's termination.

In preparation for the 10:00 a.m. meeting, Sumi jots down these notes:

- Will Jessie see this incident as poor leadership on my behalf?
- Will my technical competence and credibility as CTO be questioned?
- I must confront Greg and seek accountability; the ideal scenario is termination.
- Will I be reprimanded for not following the company ISP for safe storage of credentials?

Andrew's Backstory

Andrew (Blue House Senior Accountant)

Andrew has been with Blue House for five years, starting shortly after earning a joint accounting/information technology university degree. In those five years, Andrew received two promotions and, one year ago, took on the critical payroll responsibilities. As the head of payroll, Andrew is required to manually collect and enter employees' work hours into the accounting system, something that is typically done at the office on Saturdays, to capture the entire week's data.

Professionally, Andrew's goal was to be promoted to the Blue House CTO position. Andrew had had multiple conversations with Brad, the CEO of Blue House, and was led to believe that the job was earmarked for Andrew. To celebrate the promotion, albeit early, Andrew did something uncharacteristic: took on debt to buy a new sports car as a reward for earning the new position. Andrew also threw a party for friends and family, arriving at the party in the new car. To say everyone was impressed was an understatement.

When Andrew heard that Sumi had been promoted, panic set in; there was instant regret for the car purchase, which would be impossible to keep up without the anticipated increase in salary. The more Andrew thought about the situation, the more unfair it felt. Andrew had an accounting degree, but Sumi did not. Andrew knew about ERP systems in depth, while Sumi was an amateur.

This was when Andrew thought about the payroll system. Andrew realized that by entering "ghost" employees into the system and funneling the money back to a personal account, the car and impressive lifestyle could be kept. It was a perfect plan, especially since the payroll was entered manually.

Just in case, Andrew began building a cover story, telling Jessie, the CFO, that Sumi was underqualified for the position. Andrew felt these statements would help keep the spotlight elsewhere, help build a friendship with Brad, and paint Sumi as an employee whom Blue House should not have confidence in.

Jessie's Backstory

Jessie (Blue House Chief Financial Officer)

Jessie, recently hired as Blue House's CFO, has a passion for "numbers" that led to a degree in accounting and finance and experience in larger corporations. This is the first CFO role for Jessie in a smaller company, overseeing its financial direction. Jessie meets monthly with each director to maintain smooth operations. In the most recent meeting, Sumi proposed upgrading and integrating the AIS and MRP systems and suggested hiring Lakers Consulting to lead the project. Sumi also mentioned that, during preparation for the meeting, a few names appeared on the old payroll that had no corresponding HR or timekeeping log entries. Sumi emphasized the importance of a deeper investigation with Jessie once the upgrade is complete. Jessie has worked with Lakers Consulting before and is not 100% confident that this upgrade will be completed successfully. In the past, Jessie had been involved in project teams with Lakers Consulting, where projects did not run smoothly. Jessie appreciates Miranda, Lakers' CTO and Managing Partner, but found it difficult to work with Greg. Jessie noticed that Greg often made impulsive decisions and sacrificed accuracy for speed, frequently letting errors slide. Jessie was willing to give Lakers Consulting another chance on the ERP upgrade only because Sumi recommended the firm.

On Sunday afternoon, when the system upgrade had stalled, Sumi contacted Jessie. Sumi reported that the upgrade had frozen and that the upgrade team had an idea of what caused the stall but needed help from technical support to continue with the upgrade. Sumi reported the stall because, given the situation, the manufacturing floor would not be able to operate first thing on Monday morning. As CFO, Jessie would have to calculate the costs associated with a shutdown: the parts not produced, the employees who would still be paid even if they could not work, and the additional extra costs that would all certainly add up to a significant loss.

Jessie was furious not only because of the loss but also because of the embarrassment of the failed project. Jessie had ultimate responsibility for the project, having agreed to use Lakers Consulting. There was concern that the project could damage the professional reputation with Brad, the CEO. Jessie planned to arrive at Blue House on Monday morning and stay under the radar until full information regarding the shutdown was available.

Brad's Backstory

Brad (Blue House Chief Executive Officer)

Brad has been CEO of Blue House for only six months. Brad's father, the founder of Blue House, had an unexpected stroke eight months ago, making it necessary for Brad to leave a lucrative position at a top consulting firm to step in and lead Blue House.

As CEO, Brad has had a lot to take in. Brad's father was owner and CEO for over 30 years, which is a lot of history to understand. In assuming the CEO position, Brad decided to make both short-term and long-term plans.

In the short term, Brad planned to maintain the status quo and work through all open projects and plans that had been approved before the stroke. Brad tasked every department with documenting exactly what they do and how they do it so this information can be reviewed, studied, and analyzed.

In the long term, beginning after the first year, Brad plans to look for improvements within Blue House that can save Blue House money and also make workflow and production more efficient.

Even with so much going on within the firm, Brad is committed to building relationships with all Blue House employees, as Brad's father had done for 30 years. To foster this, Brad meets and interacts with every employee, spending most mornings walking around the office and plant, greeting people, making small talk, and jumping into meetings when possible.

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