Incorporating an assignment exemplar: the what and the how

Carolyn LaMacchia, Ph.D.
Bloomsburg University of Pennsylvania

ABSTRACT

This article describes pedagogical practices that support deeper learning within an academic program. An assignment is presented that simulates the post-graduate challenge of incorporating soft skills with discipline knowledge. The assignment tasks students with investigating a new problem or opportunity using information from a variety of sources. After research, students prepare a quality presentation to report their findings. The assignment supports the development of discipline skills and soft skills including information presentation, critical thinking, and information literacy. The assignment directions include detailed requirements and a rubric. This research exams the impact of first supplementing assignment directions with an exemplar; an ideally completed assignment. Then, second, providing an exemplar of the step-by-step process that led to the creation of the ideal assignment. The article suggests a process for administering the assignment in an upper-level information technology course. The article also describes the adaptation of the assignment to other disciplines.

Keywords: pedagogy, technology education, exemplars, critical thinking, information literacy

INTRODUCTION

Higher education institutions are charged with developing graduates who master the fundamentals of a particular discipline and are capable of developing a rewarding career. Program curriculum learning objectives specify the knowledge and skills with this goal in mind. Each course includes learning objectives to implement a set of the program-level learning objectives. After completing the program, students should be prepared for that rewarding future. This is a complicated objective that requires a partnership between the faculty and the students. Faculty deliver course content and assign assessment instruments. Students participate in the content delivery then apply knowledge and skills to assignments and exams. This is article describes an assignment which challenges students to demonstrate a variety of knowledge and skills that will likely be encountered in a career setting. Although the assignment is presented in a technology course, it may be adaptable for other disciplines.

Discipline fundamentals include a wide variety of elements that are germane to a particular field including concepts like vocabulary, epistemology, processes, and standards. Research supports the need to integrate the development of discipline knowledge and soft skills (Gerstein & Friedman, 2016). Soft skills include a wide variety of elements that through self and situational awareness enable a person to make contributions in a particular field (Gronlund & Waugh, 2009). Appropriate written and verbal communication, ability to work in a team setting, stress and time management are examples of soft skills often mentioned in research (MacDermott & Ortiz, 2017).

The ability to think critically is an extremely important soft skill and is challenging to develop and measure (Brewer & Brewer, 2015). Critical thinking is a disciplined process to reach a well-informed conclusion by unemotionally analyzing and synthesizing information (Brewer & Brewer, 2015). A critical thinker removes their personal bias from the decision-making equation; a challenging task (Gerstein & Friedman, 2016). Mastering the art and science of critical thinking can be a life-long process (Brewer & Brewer, 2015).

The critical thinking process begins with a clear identification of a problem or opportunity that is under consideration. The next step is to gather the appropriate information from appropriate sources. Well-developed information literacy skills are critical to information analysis (MacDermott & Ortiz, 2017). Information literacy guides the selection and evaluation of information that will support quality decision making. In this information age, recognizing genuine problems and opportunities along with identifying reliable information sources is a daunting task (Brewer & Brewer, 2015).

New professionals need to remain relevant in their particular discipline and industry (Mahato, 2017). Post-graduate professionals sustain their relevancy through a variety of means including research, courses, certifications, conferences, and mentorships (Mahato, 2017). Graduates remain relevant in their field by applying critical thinking skills to information and situations encountered in their professional life (Mahato, 2017). Effort to remain relevant is particularly critical for Information Technology (IT) graduates. IT professionals work in a rapidly changing technology industry that serves a rapidly changing business environment. IT professionals evaluate technology solutions to problems that they were not aware they needed to address.

Like other areas of technology, this is a phenomenon in the field of cybersecurity management. New tools are developed that combine techniques from various IT disciplines, for example artificial intelligence, with traditional cybersecurity prevention solutions. In addition, as the technology landscape develops, new types of breaches appear. As an example,

preventative measures are now available to identify and thwart the incidence of cryptojacking where cyber-criminal covertly syphon technology processing resources to be compensated for resource-intensive blockchain mining. Cryptojacking is a relatively new category of cyber breaches. Considering these issues, it is very important for IT professionals to evaluate new trends and tools in the software industry and justify the need to decision makers using developed soft skills (Mahato, 2017).

This article describes pedagogical practices that support deeper learning within an academic program. An assignment is presented that simulates challenges faced by the post-graduate professional in the application of their discipline along with soft skills. Assignment presentation within the class is described. The assignment presentation incorporates pedagogical practices that support the development of discipline skills and soft skills including information presentation, critical thinking, and information literacy. The pedagogical practices apply across most disciplines. The article describes the assignment and process for administering the assignment in an IT course. Administering the assignment includes providing an exemplar, an ideally completed assignment, and demonstrating the step-by-step process that led to the creation of the ideal assignment The article discusses the adaptation of the assignment to other disciplines.

PEDAGOGY DISCUSSION AND CONTRIBUTION

Pedagogy defines the processes and techniques used to deliver educational material. There are many parts to pedagogy that vary by instructor styles, assessment, student demographics, and program/course goals (Alonso, López, Manrique & Viñes, 2008). There is general agreement that assignments require clear purpose and directions (O'Donovan, Price & Rust, 2003). After mastery of the lower-level learning, assignments should promote the higher-level skills like critical thinking and information literacy (Adams, 2015; Anderson & Krathwohl, 2001).

Assignment directions should be reviewed with students giving them the opportunity to question material and requirements (O'Donovan, Price,& Rust, 2003). This may be accomplished in both traditional and online courses through open discussion which can take many forms including class discussion, online discussion forums, and one-on-one electronic or in-person discussion (Nilson & Goodson, 2018). Research demonstrates that active student participation in assignment discovery promotes student motivation and provides valuable feedback for the evolution of the assignment directions (Nilson, 2016). When possible, assignments should include multiple intermediate deliverables (Svinicki & McKeachie, 2014). This is particularly appropriate when an assignment includes multiple steps that have dependencies (Svinicki & McKeachie, 2014). With multiple deliverables, instructors have an opportunity to adjust a student's understanding of the assignment and also enforce quality standards (Angelo, 2012). Students tend to perform to the level of expectation (Angelo, 2012).

Exemplars serve as an illustration of a completed assignment based on a set of assignment directions. Incorporating the use of exemplars is a method for supporting student understanding of assignment directions and expectation of effort (Scoles, Huxham, & McArthur, 2013). The directions for complex assignments are more understandable when students are provided the opportunity for reviewing a completed assignment (Scoles, Huxham & McArthur, 2013). Review and discussion of a completed assignment supports expectations and compliments the expectations of grading rubrics (Sadler, 2005).

This research exams the combination of providing an ideal completed assignment (exemplar) with a step-by-step demonstration to the students of the process that led to the creation of the assignment. The assignment purpose is to simulate challenges faced by an IT professional. Career demands may place the professional into situations where they are evaluating unfamiliar material and need to draw upon their knowledge of a discipline along with their critical thinking and information literacy skills. It is theorized that students will benefit not only from viewing a completed assignment but also from the presentation of the execution of critical thinking and information literacy skills that led to the creation of the completed assignment. To support the learning process, the assignment includes three deliverables that provide intermediate feedback in support of the final assignment submission.

ASSIGNMENT DISCUSSION

Overview

Students select a topic from an internationally recognized organization's event with industry and academic participants. Event topics are related to a particular discipline. Students supplement the information with research from scholarly sources. After synthesizing the information from the event with the peer-reviewed research, students prepare and deliver a presentation on the topic that is appropriate for a corporate environment. The assignment includes intermediate deliverables including: topic selection, presentation outline, presentation slides. The final deliverable is the presentation. Through the assignment, students have a learning opportunity within a discipline and soft skills including critical thinking (information literacy: research), communication (presentation media preparation, presentation delivery), and APA formatting of reference. Refer to Exhibit 1 (Appendix) for assignment directions, presentation guidelines, and grading rubric. The assignment includes a grading rubric which sets evaluation standards and may serve as a checklist for a student to assess their own assignment prior to submission (Panadero & Jonsson, 2013; Reddy & Andrade, 2010). This assignment relates to a technology field; specifically, establishing a secure cybersecurity environment.

Learning Objective Discussion

In the evolving technological environment, Information Technology (IT) professionals must continue investigating new tools and management processes after graduation (Gerstein, & Friedman, 2016). This requires the development of multiple skills so that the IT professional can positively support the strategic direction of their organizations. The phenomena of an evolving environment applies to many professions (Gerstein & Friedman, 2016). The purpose of this assignment to evaluate a variety of cybersecurity solutions that likely have not been discussed in class. Students identify functions, compare and contrast solutions, and make a recommendation to executive management. It is intentional that these cybersecurity solutions have not been discussed in class at the start of the assignment so that students may practice the art of investigation while building critical thinking and information literacy skills as they investigate problems and opportunities in the information technology field.

The SysAdmin, Audit, Network and Security (SANS) Institute is an international organization for the advance of the cybersecurity management practices. Accredited by the Middle States Commission on Higher Education, academics and industry professionals alike participate in SANS Institute activities (SANS, 2022). The SANS Institute offers multiple

resources to support cybersecurity practitioners including an annual Summit on various cybersecurity topics (SANS, 2022). Summit focus areas include broad categories such as cloud security, industrial control systems security, and penetration testing (SANS, 2022). The SANS Institute Summits were selected for this assignment because the information presented at a summit may or may not be from a peer-reviewed scholarly source. Technology vendors and industry consultants are typically presenters at the SANS Institute Summits (SANS, 2022). These industry participants describe new advances in the cybersecurity tools and processes. IT professionals must be prepared to critically analyze information from multiple sources. While vendor information is useful. IT professionals need to recognize marketing promotional information and unemotionally analyze and synthesize information (MacDermott & Ortiz, 2017; Mahato, 2017). An assignment which includes the evaluation and synthetization of both referred information and industry information provides an opportunity for students to apply the critical thinking skill of information literacy. Student collect and ready the relevant information so that they have content for the preparation of a presentation.

IT professionals must be prepared to share ideas and discoveries in professional settings. This assignment requires the preparation and delivery of a presentation based on well-researched content (Angelo & Cross, 1993). Although students likely encounter presentation creation and delivery in multiple classes, a discussion and demonstration of the requirements can contribute to the continued development of their soft skills even if this is repetitive (MacDermott & Ortiz, 2017). Based on experience with this assignment, it is recommended that presentation guidelines be included in the project directions along with a discussion and demonstration.

Teaching Notes

In order to emphasize the assignment learning opportunities, the process for completing the assignment is demonstrated to the students. This extends the concept of providing an exemplar. Student not only review a quality completed assignment but they witness the creation of the assignment. The complete process from selection of the topic to the delivery of the presentation is demonstrated by the instructor in a traditional class or through videos, as an example, in an online class. Students participate in the discussion of each activity. Research supports the encouragement of student questioning to reinforce learning and increase motivation (Nilson, 2016; O'Donovan, Price & Rust, 2003). Refer to Exhibit 2 (Appendix) for Teaching Notes which include a schedule of activities. Steps are performed in sequence over several classes. It is recommended that there not be long gaps between class discussion and demonstration of each step. In addition, the exemplar should be shared early in the semester as students begin working on the assignment.

IMPLEMENTATION RESULTS AND CONSIDERATIONS

This assignment was developed then administered to students over the three semesters. This is an upper level course with junior and senior standing students. All students are majoring or minoring in technology. For the initial delivery, Trial 1, the assignment directions were shared and discussed with the students. The second delivery, Trial 2, the assignment directions were again shared and discussed with the students, as in Trial 1. Delivery of Trial 2 also included the exemplar. Exhibit 3 (Appendix) includes the exemplar presentation text. Delivery of Trial 3

followed the same process as Trial 2 with the addition of the demonstration of the process to create the exemplar. In summary:

- Trial 1 – Assignment directions shared with students.
- Trial 2 – Assignment directions shared with students.
  Exemplar presentation shared with students.
- Trial 3 – Assignment directions shared with students.
  Exemplar presentation shared with students.
  Exemplar process shared with students.

A comparison was made of the results of each assignment trial based on rubric data. The scores in Figure 1 (Appendix) are the average points that the class earned in each category criterium. In calculating a student's grade, the Content assignment category is weighted twice the weight of the Organization and Presentation categories. To facilitate comparison in this study, the points in the Content assignment category were halved so that the points are on the same scale as the Organization and Presentation categories.

Considering all three trials, there was little change in performance for rubric categories that required following assignment directions. All three trials included the distribution of detailed assignment directions coupled with class discussion. The detail assignment directions included presentation guidelines as well as the grading rubric. Content categories involving business terminology and presentation timing show little change. These are criteria numbers Con4 and Con5. Organization categories involving presentation introduction, APA formatting of references, and best practice in slide creation show little change. These are criteria numbers Org1, Org4, and Org5. Presentation categories dealing with the use of slang and relying on presentation support materials show little change. These are criteria numbers Pre3 and Pre5. It may be theorized that the incorporation of an exemplar presentation and an exemplar process demonstration may not impact these criterium of student performance. In other words, detailed assignment directions that include presentation standards and grading rubric are sufficient for these criterium of student performance.

Considering the progression through each trial, there was improvement shown in Content categories involving accuracy of information, research effort, and recognizing marketing promotional information. There are criteria numbers Con1, Con2, and Con3. Organization categories involving presentation content transitions and accurate conclusion showed improvement. These are criteria number Org 2 and Org 3. Presentation category dealing with speaker poise, vocalization, and sentence structure showed improved. These are criteria numbers Pre1, Pre2, and Pre4. It may be theorized that the incorporation of an exemplar presentation and an exemplar process demonstration may have impacted these criterium of student performance where the largest improvement in scores can be observed between Trial 1 and Trial 3. In general, students performed better during Trial 3 for all three categories of rubric criterium.

After Trial 2 and 3 of the assignment, the experience with the exemplar was discussed with students. Student comments included:

1. Instructions are much clearer after seeing the example.
2. Instructions are much clearer with seeing the process to create the example.
3. I'm a bit intimidated about expectations of me after seeing the instructor's presentation.
4. It was helpful when marketing information with the summit information was highlighted.
5. Some of the summit presentations are entertaining and helped me focus.

6. Seeing the completed assignment and discussion how it was made makes more sense to me than feedback on the assignment deliverables.

The results of this study are comparable to studies involving the addition of exemplars. As in these studies, an exemplar is another resource to support student performance. This student also suggests that an exemplar of the process to create the ideal assignment also supported student performance.

It is important to recognize that the classes in Trials 2 and 3 included more senior students. It can be argued that senior students are further in their development of both discipline knowledge and soft skills. Admittedly, the creation of the exemplar can be time consuming. And, in many disciplines, the exemplar may quickly become outdated so frequent recreation of the exemplar is required.

CONCLUSION

An assignment is presented that simulates challenges faced by the post-graduate professional in the application of discipline skills and soft skills. Pedagogical practices are described in the delivery of the assignment in either a traditional or online course. The pedagogical practices support the development of discipline skills and soft skills including information presentation, critical thinking, and information literacy. The pedagogical practices apply across most disciplines. The article presents an assignment and process for administering the assignment in an IT course. The assignment was delivered in three semesters. A comparison was made of the rubric results to detect improvement in class results. The practice of providing an exemplar assignment and the process of creating the exemplar assignment appears to contribute positively to class performance.

The assignment and process may be adapted to other disciplines. The adapted assignment references an organization which sponsors an event that includes vendor representatives. This provides students the opportunity to critically evaluate information from the event with information discovered through academic research.

REFERENCES

Adams, N. E. (2015). Bloom's taxonomy of cognitive learning objectives. *Journal of the Medical Library Association*, 103(3), 152-153.

Alonso, F., López, G., Manrique, D., & Viñes, J.M. (2008). Learning objects, learning objectives and learning design. *Innovations in Education and Teaching International*, 45(4), 389-400.

Anderson, L. W., & Krathwohl, D. R. (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. White Plains, NY: Longman.

Angelo, T. A. (2012). Designing subjects for learning: Practical, research-based principles and guidelines. In L. Hunt & D. Chalmers (Eds.), *University teaching in focus: A learning-centered approach* (pp. 93–111). Melbourne, Australia: ACER Press.

Angelo, T. A., & Cross, K. P. (1993). *Classroom assessment techniques: A handbook for college teachers* (2nd ed.). Jossey-Bass.

Brewer, P. E., & Brewer, E. C. (2015). Pedagogical perspectives for the online education skeptic. *Journal on Excellence in College Teaching, 26(1),* 29–52.

Fakiha, B. S. (2020). Effectiveness of Security Incident Event Management (SIEM) System for Cyber Security Situation Awareness. *Indian Journal of Forensic Medicine & Toxicology*, 14(4), 802–808.

FireEye. (2019). FireEye Launches Purple Team Assessments to Test Security Operations With Mandiant Experts. *Business Wire* (English).

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, 21(3267), 3267.

Gerstein, M., & Friedman, H. H. (2016). Rethinking higher education: Focusing on skills and competencies. *Psychosociological Issues in Human Resource Management*, 4(2), 104-121.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors* (Basel, Switzerland), 21(14).

Gronlund, N. E., & Waugh, C. K. (2009). *Assessment of student achievement* (9th ed.). Upper Saddle River, NJ: Pearson.

Guneysu, S. (2021). Designing Playbooks with Purple Team Approach, Purple Team. *SANS Summit & Training 2021*, May 17, 2021.

MacDermott, C., & Ortiz, L. (2017). Beyond the Business Communication Course: A Historical Perspective of the Where, Why, and How of Soft Skills Development and Job Readiness for Business Graduates. *The IUP Journal of Soft Skills*. 11. 7-25.

Mahato, P. C. (2017). Campus to corporate: Learn, adapt, change, and survive. *ICFAI Journal of English Studies*, 12(1), 95-97.

Medin, T. (2019). Keynote Purple Yourself, Purple Team. *SANS Summit & Training 2019*, October 21, 2019.

Nilson, L. B. (2016). *Teaching at its best: A research-based resource for college instructors* (4th ed.). Jossey-Bass.

Nilson, L. B., & Goodson, L. A. (2018). *Online teaching at its best: Merging instructional design with teaching and learning research*. Jossey-Bass.

O'Donovan, B., Price, M., Rust, C. (2003). Improving students' learning by developing their understanding of assessment criteria and processes. *Assessment and Evaluation in Higher Education*, 28(2), 147–164.

Outkin, A. V., Schulz, P. V., Schulz, T., Tarman, T. D., & Pinar, A. (2021). Defender Policy Evaluation and Resource Allocation Using MITRE ATT&CK Evaluations Data. *Cornell University ARzIV*, 2107.04075.

Owens, D. (2021). Threat Focused Purple Team Exercise (non-AD Edition), Purple Team. *SANS Summit & Training 2021*, May 17, 2021.

Panadero, E., & Jonsson, A. (2013). The use of scoring rubrics for formative assessment purposes: A review. *Educational Research Review, 9*, 129–144.

Ponemon Institute. (2018). Cost of a Data Breach Study: Benchmark Research sponsored by IBM Security, independently conducted by Ponemon Institute, LLC, July 2018.

Reddy, Y. M., & Andrade, H. (2010). A review of rubric use in higher education. *Assessment & Evaluation in Higher Education, 35,* 435–448.

Rogers, M. (2020). Purple Team Feedback Loop. *SANS Cyber Solutions Fest 202*, October 8, 2020.

SANS. (2022). SANS Technology Institute. Retrieved from: https://sans.edu

Scoles, J., Huxham, M., & McArthur, J. (2013). No longer exempt from good practice: Using exemplars to close the feedback gap for exams. *Assessment & Evaluation in Higher Education*, 38(6), 631–645.

Svinicki, M. D., & McKeachie, W. J. (2014). *McKeachie's teaching tips: Strategies, research, and theory for college and university teachers (14th ed.)*. Belmont, CA: Wadsworth.

Wittkop J. (2016). *Incident Response Planning. In: Building a Comprehensive IT Security Program*. Apress, Berkeley, CA.

Wood, R. & Bengtson, W. (2016). The Rise of the Purple Team. *RSA Conference 2016*, San Francisco, CA.

APPENDIX

Exhibit 1: Assignment Directions.

Purpose:

In the evolving technological environment, Information Technology (IT) professionals must continue investigating new tools and management processes after graduation. This requires the development of multiple skills so that the IT professional can positively influence their organizations. The purpose of this assignment to evaluate a cybersecurity solution(s) that have not been discussed in class. Identify functions, compare and contrast solutions, and make a recommendation to executive management about the viability of the solution. It is intentional that these cybersecurity solutions have not been discussed in class at the start of the assignment so that students may practice the art of investigation.

Requirements:

1. Select a topic from SAN's Institute Virtual Summits.

➔Submit topic selection to assignment drop box before the due date. Student will receive feedback.

2. Research the topic from the viewpoint of several reliable sources including the university library, Google Scholar, and major vendors.
3. Based upon research, develop a background in the topic. Be able to describe the topic, provide its purpose, discuss the advantages and disadvantages, describe challenges, and make recommendations for appropriate implementation.
4. Formulate logical questions about the topic based upon research.
5. Complete a review of the summit information on the topic.
6. Outline the presentation based on a review of the materials.

➔Submit outline and references in APA format to the assignment drop box before the due date. Student will receive feedback.

7. Develop slides following professional guidelines (refer to directions).

➔Submit slides to the assignment drop box. Student will receive feedback prior to presentation. Student should incorporate feedback into slides prior to class presentation.

➔ 8. Present to class based on posted presentation schedule.

Presentation Guidelines:

Design with a recognition of the purpose of the presentation and knowledge of the audience.

Presentation Organization:

Organize the delivery to include an agenda, introduction, presentation body, and conclusion. Each is described below.

Introduction
Capture attention
Establish credibility
Preview main points

Presentation body
Develop two to four main points
Streamline and summarize principal parts of each point
Arrange information logically

Conclusion
Summarize main themes
Conclude with a recommendation
Leave the podium gracefully.

Visuals (Slides) Preparation:

Focus on major concepts only because presenter fills in details with voice.
Consistency in appearance
Readability of text, graphics, background colors
Include graphics; too many reduces effectiveness.
Animations should be used sparingly and not interrupt the flow of the verbal presentation.
All hyperlinks should work.
Slides are numbered so that viewer can refer to a specific slide during question/answer session.

Keep Slides Simple
Paraphrase with "bulleted" items – no paragraphs
Observe 6-x-6 (or 7-x-7) rule
    Less than or equal to six words per line
    Less than or equal to six lines per slide
Visually appropriate and relevant background, clip art, vides, and graphics
Honor copyright to material included in slides

Verbal Presentation Supported with Slides:

Build rapport with imagery or anecdote
Select vocabulary/words wisely
Voice control considers volume and tempo
Avoid filler words (like, um, you know)
Thoughtfully present data and statistics – round numbers
Include verbal signposts: preview, summarize, switch directions
Speak extemporaneously without reading slides or note cards
Move around the presentation area (if possible)
Vary facial expressions
Use eye contact

Rehearse presentation. Prepare for not knowing an answer to a question raised by the audience. Practice presentation for optimal performance (one hour of practice for every presentation minute)

Grading Rubric				
Content (Con)	**Points:**	**2**	**6**	**8**
No.	**Criteria**	**Deficient**	**Meets**	**Exceeds**
Con1	Information is completely accurate; facts are precise and explicit.			
Con2	It is evident that the student researched the topic; brought in personal ideas and information to enhance the discussion.			
Con3	A distinction is made between marketing promotional information and referred information.			
Con4	Appropriate business and technical terminology are used.			
Con5	Presentation is as long as it needs to be; no time-fillers. Presentation should not exceed 20 minutes.			
Organization (Org)	**Points:**	**1**	**3**	**4**
No.	**Criteria**	**Deficient**	**Meets**	**Exceeds**
Org1	Presentation includes an accurately crafted introduction.			
Org2	Presentation content transitions logically as topics change; telling an effective story.			
Org3	Presentation includes an accurately crafted conclusion.			
Org4	Presentation includes references in APA format as the last slide(s).			
Org5	Slides follow best practice as presented in the assignment directions.			
Presentation: (Pre)	**Points:**	**1**	**3**	**4**
No.	**Criteria**	**Deficient**	**Meets**	**Exceeds**
Pre1	Speaker is poised and uses clear articulation, proper volume, appropriate rhythm, enthusiasm confidence, eye contact. It is clear that the presentation was practiced.			
Pre2	Speaker uses precise pronunciation of terms and incorporates rich and varied words for context.			
Pre3	Presentation is free from slang.			
Pre4	Presentation uses appropriate sentence structure and organization.			
Pre5	Presenter does not rely on video(s) developed by others or note cards. Presenter does not read slides.			

Exhibit 2: Teaching Notes

1 – Discuss the organization and the event. Select a topic for the exemplar which will be demonstrated by the instructor. Students will select their own topic which is approved by the instructor as part of the assignment directions.

2 – Research the topic from the viewpoint of several reliable sources including the university library, Academic Associations/Institutions, Google Scholar, and major vendors. The instructor demonstrates research processing and the gathering of references in APA format.

3 – Based upon research, develop a background in the topic. Be able to describe the topic, provide its purpose, discuss the advantages and disadvantages, describe challenges, and make recommendations for appropriate implementation. The instructor addresses the background of the exemplar topic with the class.

4 – Formulate logical questions about the topic based upon research review in Steps 2 and 3. For example, what tools are available to address an issue. How can the issue be best managed?

5 – Complete a cursory review of organization's material available on the exemplar topic. Review abstracts, videos, white papers, etc. Reach a conclusion on the appropriate materials of interest from totality of material available on the topic. The instructor describes their review process of the topic based on the organization's materials.

6 – Outline presentation. The instructor outlines the presentation of the exemplar topic and discusses logic behind outline entries.

7 – Fill-in presentation outline with sources from Steps 2 and 5. Share the results with the students and discuss thought process.

8 – Develop slides following professional guidelines. Critique the slides based on the best practice recommendations included in the assignment.

9 – Present the presentation to the class. Tell a story of the topic. Critique the presentation delivery based on best practice recommendations included in the assignment.

Exhibit 3: Exemplar Presentation Text. Graphics eliminated for brievity.

<u>Slide 1 - Project Introduction</u>

- Cybersecurity environment
  - Complex
  - Appropriate management is critical
- The SysAdmin, Audit, Network, and Security (SANS) Institute[1]
  - For-profit private company founded in 1989
  - Annual summits on various cybersecurity topics
- Purple Team ←FOCUS

[1](SANS, 2022)

Slide 2 – Management

Manager

- Leader and Communicator
- Impacted by organizational structure
    - Different agendas
    - Different objectives

Cybersecurity Management[1]

- Art and Science:
- Cross-domain knowledge
    - People + Technology + Process

[1](Wittkop, 2016)

Slide 3 - Problem / Opportunity

- Breaches[1]
    - Frequency
    - Damages
    - Detection
        - Average - six (6) months
- Tools and Hardening do not guarantee infrastructure safety[2]
- Evolving Development Environment[2]
    - Problems are opportunities
    - Frameworks – "how to"
    - Tools – "Prevention and Detection"

[1](Ponemon Institute, 2018).

[2](Wittkop, 2016).

Slide 4 – Management Response[1]

Separate teams established (2003)

- Different agendas, objectives, leadership
- Operate in a vacuum within/between team
- Feedback/reports not shared
- Credibility of audits is impacted (contradicting nature of teams)

Red Team

- Offensive hacker
- Success dependent on how many controls the team can bypass (Blue team failure points)

Blue Team

- Defensive hunter
- No alerts = preventative controls all worked
- A lot of alerts mean that detection capability is firing on all cylinders.

[1](Chowdhury, 2019)

Slide 5 - Purple Team – Red + Blue

Originated in 2016[1, 2, 3, 4]

- Not well-understood
- Re-organization of separate teams

White (Documentation varies on "white" role.)

- White color mixed with red and blue, maintains purple color.
- Develops core philosophy
- Manages missions
- Translate technical finds to actional items

Red

- Offensive
- Hacker

Blue

- Defensive
- Hunter

[1](Chowdhury, 2019)
[2](Owens, 2021)
[3](Wittkop, 2016)
[4](Wood & Bengtson, 2016)

Slide 6 - Implementation of Purple Team[1, 2, 3, 4, 5]

White Team leads testing plans

- Identify "Crown Jewels"
- Assume breach is in-progress
- Reviews test results
- Categorize and prioritize issues identified

Red makes Blue better

- Not adversaries
- Failures are learning opportunities
- Joint effort
- Results reported as a team
- Create matrix to categorize urgency and complexity to fix vulnerabilities

[1](Guneysu, 2021)
[2](Medin, 2019)
[3](Rogers, 2020)
[4](Wittkop, 2016)
[5](Wood & Bengtson, 2016)

(continued)

Slide 7 – Comparion
Without Purple Team

- Knowledge barriers
- Duplication of effort
- Silos
- Limited ROI
- Slower response during an incident
- Detection/analysis gaps
- Job transition challenges

Slide 8 - Comparison (continued)
With Purple Team

- Focus on strengths
- Defined roles and responsibilities
- Collaborative environment
- Additional opportunities for ROI
- More efficient response efforts
- Stronger detections and analysis
- More training leading to career opportunities

Slide 9 - Implementation: Framework Tool Discussion[1, 2]
MITRE ATT&CK®

- MITRE: Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).
- Tool for simulating cybersecurity breaches.
- Customizable for various technology environments.
- Consider a resource for Purple Team activities.

[1]Georgiadou, Mouzakitis & Askounis, 2021)
[2]Outkin, Schulz, Schulz, Tarman & Pinar, 2021)

Slide 10 - Implementation: Application Discussion[1, 2]
SIEM

- Security Information and Event Management (SIEM).
- Holistic view of information security.
- Real-time visibility across a system
- Respond appropriately to identified threats
- Example: Event log management that consolidates data from numerous sources.

[1](Fakiha, 2020).
[2](González-Granadillo, González-Zarzosa & Diaz, 2021).

(continued)

Slide 11 - Implementation: Application Discussion[1]

FireEye Mandiant® Services

- Recreate cyber-attacks with short or long-term durations.
- Reports Purple Team's progress on discovering, mitigating, and repairing breach.
- Generates detailed score card with quantifiable recommendations.

[1](FireEye, 2019).

Slide 12 - Conclusion

- SANS Summit Presentations
  - Informative and entertaining
  - Target audience should have some familiarity with topic
- Appreciate manager's role
  - Impacted by organizational structure
- Purple Team
  - Described it
  - Discuss implementation
- Developed decision making skills
  - Preliminary research
  - Cautious evaluation of for-profit advice
- Improve understanding of assignment? Share thoughts.

Slides 13 and 14– References

References provided to students in APA format. Not repeated here.

Table 1

Trial sizes by class standing.

TRIAL	Junior	Senior	Total	Percent of Senior
1	11	19	30	63.33
2	9	25	34	73.53
3	7	19	26	73.08

Table 2
Average class results by rubric criterium by trial. Note: For analysis Content scores halved.

No.	Trial 1	Trial 2	Trial 3
Con1	2.3	2.8	3.1
Con2	2.7	2.9	3.2
Con3	2.3	3.0	3.2
Con4	2.9	3.0	3.0
Con5	3.0	3.0	2.9
Org1	2.9	2.8	3.0
Org2	2.6	2.9	3.0
Org3	2.6	2.9	3.2
Org4	2.9	2.9	3.0
Org5	2.8	2.9	2.9
Pre1	2.9	3.0	3.2
Pre2	2.6	3.0	3.1
Pre3	2.9	3.0	3.0
Pre4	3.0	2.9	3.4
Pre5	3.0	2.9	3.1

Table 3
Change in average class results by rubric criterium between trials.

No.	**Change from Trial 1 to Trial 2**	**Change from Trial 1 to Trial 3**	**Change from Trial 2 to Trial 3**
Con1	0.5	0.8	0.3
Con2	0.2	0.5	0.3
Con3	0.7	0.9	0.2
Con4	0.1	0.1	0.0
Con5	0.0	-0.1	-0.1
Org1	-0.1	0.1	0.2
Org2	0.3	0.4	0.1
Org3	0.3	0.6	0.3
Org4	0.0	0.1	0.1
Org5	0.1	0.1	0.0
Pre1	0.1	0.3	0.2
Pre2	0.4	0.5	0.1
Pre3	0.1	0.1	0.0
Pre4	-0.1	0.4	0.5
Pre5	-0.1	0.1	0.2

Figure 1: Average Results by Criterium by Trial

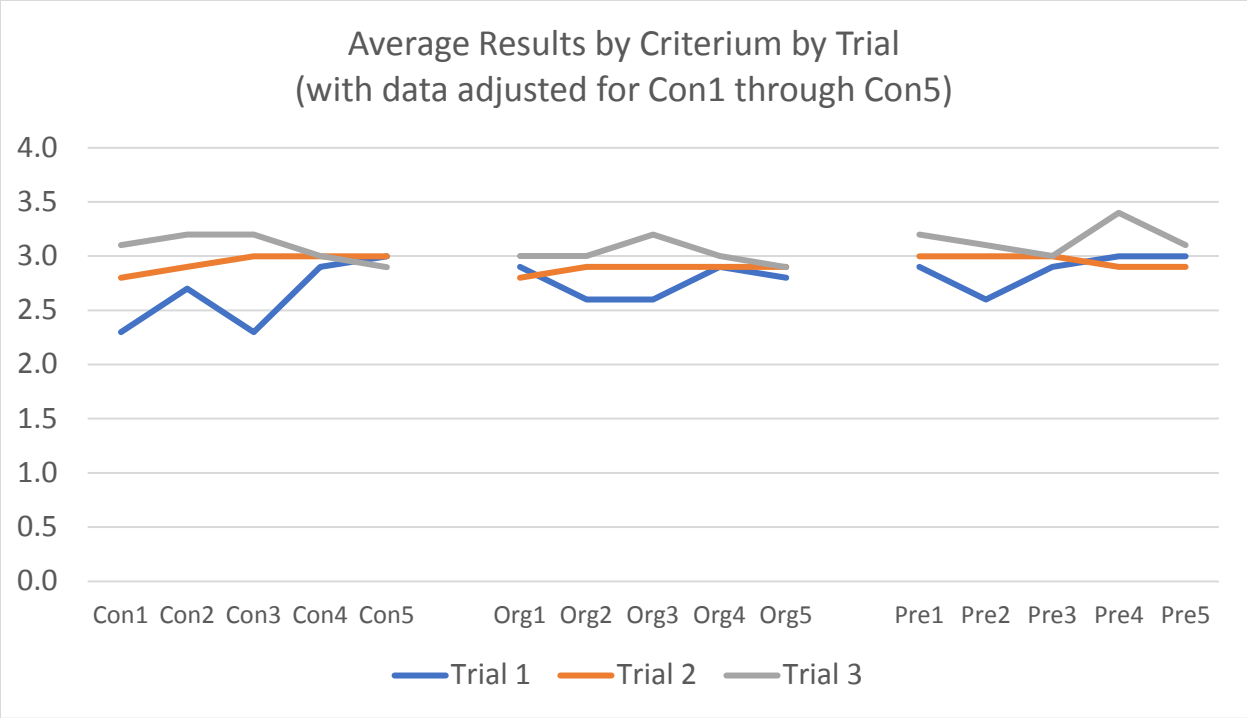

Figure 2: Change in Results between Trials.