BSCSIA Course Kick Start Guide– C841

Course Applicability: C841, Legal Issues in Information Security

This course addresses the laws, regulations, authorities, and directives that inform the development of operational policies, best practices, and training to assure legal compliance and to minimize internal and external threats. Students analyze legal constraints and liability concerns that threaten information security within an organization and develop disaster recovery plans to assure business continuity.

Prerequisite Courses: C836 is strongly recommended

Typically, successful students complete the course in ~**46 days.**

About This Guide

This Kick Start Guide can be used as supplemental resource to help you get started with the course, get answers to frequently asked questions, and be leveraged to help with completing the performance assessment for the course. You can find the primary course material for the course by clicking the "Go To Course Material" button on your course page. Reach out to your assigned course instructor for additional guidance once assigned.

Guide Contents

What's Required to Complete the Course

What to Produce

The course has two tasks (Task 1 and Task 2) that must be completed and passed for you to complete the course. You must provide sufficient responses to the questions in each task using a file within the file restrictions section of your task requirements. You will submit only one file per task and may submit them in any order. You do not have to wait for one task to pass before submitting the other. The most common submissions are in the form of a .ppt or .doc document.

File Restrictions
*File name may contain only letters, numbers, spaces, and these symbols: ! - _ . * ' ( )*
File size limit: 200 MB
File types allowed: doc, docx, rtf, xls, xlsx, ppt, pptx, odt, pdf, txt, qt, mov, mpg, avi, mp3, wav, mp4, wma, flv, asf, mpeg, wmv, m4v, svg, tif, tiff, jpeg, jpg, gif, png, zip, rar, tar, 7z

Page/Word Count and Formatting

Page/Word Count Minimum and Format

There is **no specified minimum or maximum page or word count** requirement for the tasks. You should simply look to provide complete responses to each question that satisfy what the task requirements and rubric calls for.

There is **no specific formatting or writing style** such as APA, MLA etc. requirement. You should however, format your work using section headers that correlate to the specific task requirements/rubric points. Provide your responses to the specific task requirement points in the corresponding section of your work.

Format Recommendations: (1) Select the type of document you want to use (.doc, .ppt etc.), (2) create a title page containing your name, the course, and task number at minimum, and (3) include section/paragraph headers for each question (i.e. a header called "*A1*", or "*CFAA and ECPA*" as the header for Task 1 section A1). Provide the response to that section under the corresponding header in your work. Continue on the same path for each section of the task. Conclude with a references page ***if*** you cited any material in your work.

Performance Assessments and Originality and Similarity Standards

Performance Assessment Basics and Unicheck

Need help getting started with your Performance Assessment, view the video Planning & Pre-writing a Performance Assessment, and the WGU Knowledge Center article Performance Assessment Submission, which covers assessment submission from start to finish.

Your submission must be your original work. No more than a combined total of ***30%*** of the submission and no more than a ***10%*** match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly. View Video linked here for similarity check procedures: ***Video on Reviewing Unicheck Reports-**

Sources and Citations FAQ

Sources and Citations Requirements

Q: Do I have to include in-text/in-line citations in my work?

A: No, you do not. However, **IF** you choose to quote, paraphrase, or summarize content from a source, **THEN** you must acknowledge that source using in-text/in-line citations and an accompanying reference page/reference slide. Your work can be 100% original work if you choose.
The one area from the entire assignment, where you may not be able to get around keeping your work fully original is Task #2 Part A1/A1a where you are asked to provide specific ethical guidelines used by other organizations. Since those guidelines will be those organizations' content, best practice to capture them would be for you to directly quote/paraphrase/summarize them.

Q: If I quote, paraphrase, or summarize content from a source, do I have to use APA format?
A: No, you do not. There is no specific writing style requirement for the assignment. This absence of a standard writing style, however, introduces ambiguity in what information is required for citations and reference lists that often leads to task returns for missing information. So, if you choose to quote, paraphrase, or summarize content from a source you should look to, at a minimum, include the core elements of **author, date,** and **title** for your citations and accompanying reference lists. A safe bet is to just optionally employ APA, or another style for the citation and references portion of your work regardless of how you format the whole work.

Q: If I want to quote, paraphrase, or summarize content from a source, where can I get help with formatting the citations and references?
A: There is no specified writing style you must use for the assignment, but there is a plethora of information on APA citations and references within the WGU Writing Center.

Q: I would like to quote, paraphrase, or summarize content from the course text to support one of my responses, where do I find the author and date information to acknowledge the text?
A: This information can be found on page 2 of the text. I have pasted it here for quick reference as well.
Grama, Joanna Lyn. (2015) Legal Issues in Information Security

Q: I would like to quote, paraphrase, or summarize content from the case study to support one of my responses, where do I find the author and date information to acknowledge the case study?
A: Use a no author, no date annotation for your citation i.e. (TechFite Case Study, n.d.) and a no date, no author with a "retrieved from" link for your reference page entry. i.e., TechFite Case Study, n.d. Retrieved from [copy/past task page URL where case study resides here]

Q: How much of my work can be quoted, paraphrased, or summarized content from a source?
A: *No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source.*
Q: Is properly cited information subject to the 30% total similarity threshold?
A: Yes. Your submission can have n*o more than a combined total of 30% similarity* ***even if cited correctly****.*

	Citation and Reference Example 1-No Specific Writing style
In-text	An ethical guideline used by the Information Systems Security Association (ISSA) states that members will "Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles" (ISSA Code of Ethics, n.d.).
Reference Page entry	Information Systems Security Association (ISSA) Code of Ethics. n.d. Retrieved from https://www.issa.org/issa-code-of-ethics/

	Citation and Reference Example 2-No Specific Writing style
In-text	According to Grama (2015), "the Internet is a protected computer because the Internet facilitates commerce between different states".
Reference Page Entry	Grama, J. (2015). *Legal issues in information security*, Second Edition. Burlington, MA

Writing Center and Grammarly

WGU Writing Center

At the WGU Writing Center students will acquire the skills and resources they need to become stronger writers.

- E-mail the Writing Center at writingcenter@wgu.edu
- Click here to schedule an appointment with the Writing Center
- https://my.wgu.edu/success-centers/writing-center
- Writing Center Help Line: (877) 435-7948 x2967

Below are some additional links to help with writing performance assessments:

- Tips for Writing Performance Assessments
- Using Credible Sources
- Paraphrasing
- Citing Your Sources
- Creating a Reference Page

Case Study – All responses to your tasks must be based on activity observed in the TechFite Case Study

TechFite Case Study

Background of Company

TechFite is traded on NASDAQ and has approximately 1,000 employees. The company's core business involves consulting with and advising Internet organizations on promoting and monetizing their online business ventures. Most of the company operates legally and ethically with good internal financial oversight. However, its Applications Division has recently been reported in the news media for undertaking some disturbing business practices. This division consults with start-ups on launching new applications and apps online.

The chairperson of the board commissioned me, John Jackson, to investigate the IT and business practices of the Applications Division. I hold an MS in network security and am qualified as a Certified Information Systems Security Professional (CISSP), and I have 12 years' experience in cybersecurity. In addition, the chairperson has consented to allow Maria Harrison to assist me. She is a private investigator who holds an MS in criminal justice and has 15 years' experience in corporate investigations.

Findings

I interviewed Noah Stevenson, the chief executive officer (CEO) of Orange Leaf Software LLC, whose company was cited in recent news articles about the Applications Division. Stevenson indicated his company had meetings with the division's representatives to possibly hire TechFite for consulting services. Prior to divulging any technical details, Applications Division head Carl Jaspers executed a nondisclosure agreement (NDA) with Orange Leaf. As a part of the preconsulting process, Orange Leaf's CEO, chief technology officer (CTO), and lead software engineer completed questionnaires that included technical information about Orange Leaf's products. Ultimately, Orange Leaf decided not to hire TechFite's Applications Division for a variety of business reasons. Months later, Noah Stevenson was disturbed to find out a competitor was launching some products very similar to those of Orange Leaf.

A similar scenario occurred in an interview with Ana Capperson, CTO for Union City Electronic Ventures. She described the same fact pattern as Orange Leaf's. That is, after this company decided not to use the Applications Division, proprietary information eventually found its way into the hands of a competitor.

Both potential clients provided copies of the questionnaires to me, and they do contain information that could be of value to a competitor. Copies of the NDAs executed by Carl Jaspers were also provided. A check of the Applications Division's customer database revealed that the two competitors identified by Stevenson and Capperson are existing clients of TechFite's Applications Division.

The Applications Division has a Business Intelligence (BI) Unit, which gathers publicly available information about companies in the Internet sector to benefit the division's marketing of its services and to aid clients. Such an operation is legal and is common in the industry. However, I was interested in what kind of oversight the unit had to prevent the abuses alleged by Stevenson and Capperson.

IT Security Analyst Nadia Johnson of TechFite's Applications Division reviewed reports for the chief information security officer (CISO) and revealed the organization had performed a credible job of protecting the division's network against external threats. Vulnerability scanning, penetration testing, and UTM (unified threat management) were all in place. Documentation on internal oversight, especially of the BI Unit, however, was lacking. There were blanket summaries that no irregularities were found in internal operations. What was missing were specific discussions of auditing users' accounts, checking for escalation of privilege, enforcing data loss prevention (DLP) on sensitive documents, and surveilling internal network traffic and activity.

Also disturbing was the lack of coverage on the critical issue of safeguarding sensitive and proprietary information belonging to existing clients, potential clients, and previous clients. No plan was evident in keeping different clients' information segregated from each other and employing a Chinese wall methodology. (No general policy at TechFite requires such a methodology.) Within the BI Unit, the principles of least privilege and separation of duties were not enforced. Every

workstation and computer had full administrative rights. In the marketing/sales unit associated with the BI Unit, the same person can create customers (clients), report sales, and post sales on the system. In fact, there is no IT segmentation or separation between the two units—data or applications. Each unit has full visibility and access into the other.
Additionally, background checks into IT Security Analyst Nadia Johnson raised some questions. First, Jaspers (head of Applications Division) regularly gives Johnson's boss, the CISO, positive recommendations about Johnson during annual reviews and she gets ample raises. Johnson's social media posts have photos and text documenting her frequently attending social events hosted by Jaspers. A recent post even thanks Jaspers for a gift on Johnson's birthday. (Currently, no policy at TechFite bars social relationships between IT Security staff and those they conduct oversight on.)

We audited the client list database for the division (an action never done by Johnson). Most of the clients are well-known companies in the Internet arena. We researched the businesses we did not immediately recognize online. All but three came up as legitimate companies in the Internet field. These three organizations—Bebop Software of Alberta, FGH Research Group of Indiana, and Dazzling Comet Software of Florida—had no real Internet presence. Further investigation revealed they were all incorporated in Nevada. The registered agent for all three corporations was Yu Lee, who attended graduate school with Carl Jaspers at Stanford University.

We crosschecked with the TechFite Financial Unit and found all three companies pay for services at TechFite with checks drawn from the same bank: Freeworkers' Pennsylvania Bank, NA in Scranton, Pennsylvania. Given this pattern, these three clients may not be actual, real clients but may simply be conduits for moving money into TechFite's sales figures for the division. Since TechFite does not do business with Freeworkers and does not have accounts there, the bank may provide an off-the-books method of making payments elsewhere.

In auditing IT user accounts for the division, we found most to be created in the normal manner for TechFite. (A manager requests that an employee receives account access with the appropriate privileges.) However, two accounts were created solely upon the request of Carl Jaspers. The employees assigned to the accounts have not worked for TechFite for over a year. However, the accounts are in constant use. Emails associated with these accounts are addressed to parties who are not clients of TechFite. Some of the emails refer to intelligence-gathering activities against various companies, including references to "dumpster diving" and "trash surveillance."

All TechFite employees at the time of hire sign a release permitting company surveillance of any electronic communications using TechFite equipment. Accordingly, we remotely deployed Encase Endpoint Investigator on BI Unit computers and digital devices. We discovered the Metasploit tool (used for system penetration) on multiple machines. In addition, evidence on the hard drives indicates recent penetration and scanning activity into IP addresses for several Internet-based companies.

Among the BI Unit employees, Sarah Miller, the senior analyst, has the most traffic in scanning other companies' networks. Analysts Megan Rogers and Jack Hudson take direction from Miller in doing similar efforts. Hudson also coordinates efforts by third parties to gather intelligence through surveilling and through mining companies' trash. Furthermore, social media research on Hudson revealed his membership in the Strategic and Competitive Intelligence Professionals (SCIP), which has a very strong code of ethics against covert and illegal BI activities.
Finally, and very disturbing, the BI Unit, through its dummy user accounts, has gained access to other groups and units within TechFite outside its own division, without proper authorization. Escalation of privilege has occurred on these accounts to permit access to legal, human resources (HR), and finance departments. Networking monitoring logs reflect regular traffic between the BI Unit and these other departments to examine financial and executive documents.
[End of report]

Task Best Practices

1. Use Headers. Include a header in your submission that corresponds to each task requirement/rubric section. This can be as simple as using the alpha-numeric code or an abbreviated version of the section (i.e., A1, or CFAA and ECPA as the header for Task 1 section A1). Provide the response to that section under the corresponding header in your work.

2. Provide responses independently. Each task requirement/rubric section is evaluated independently in a vacuum so to speak. So a good approach is to provide a response to each one as if the other sections do not exist. i.e., don't write out "as previously mentioned or mentioned above" etc. Reiterate, restate, rephrase as needed to provide a separate response to each section.

3. Provide responses to answer the question, not for overall flow. Each section is evaluated as a standalone against the rubric. An essay/storyline approach often leaves actual answers to questions overlooked or hidden in paragraphs (I see many, many task returns due to this). Making your responses clear, complete, and organized under header matching rubric points the way the templates I shared are structured, makes it easy for your evaluator to find them, which makes things better for you.

4. Pay attention to tenses. Look out for items that are plural in the requirements and ensure you provide two or more where applicable. For instance, the first part of Task 1 section B1b, states "Explain how existing cybersecurity policies…". Here you would be mindful not to overlook the word "policies" being plural and discuss two or more of them in your response.

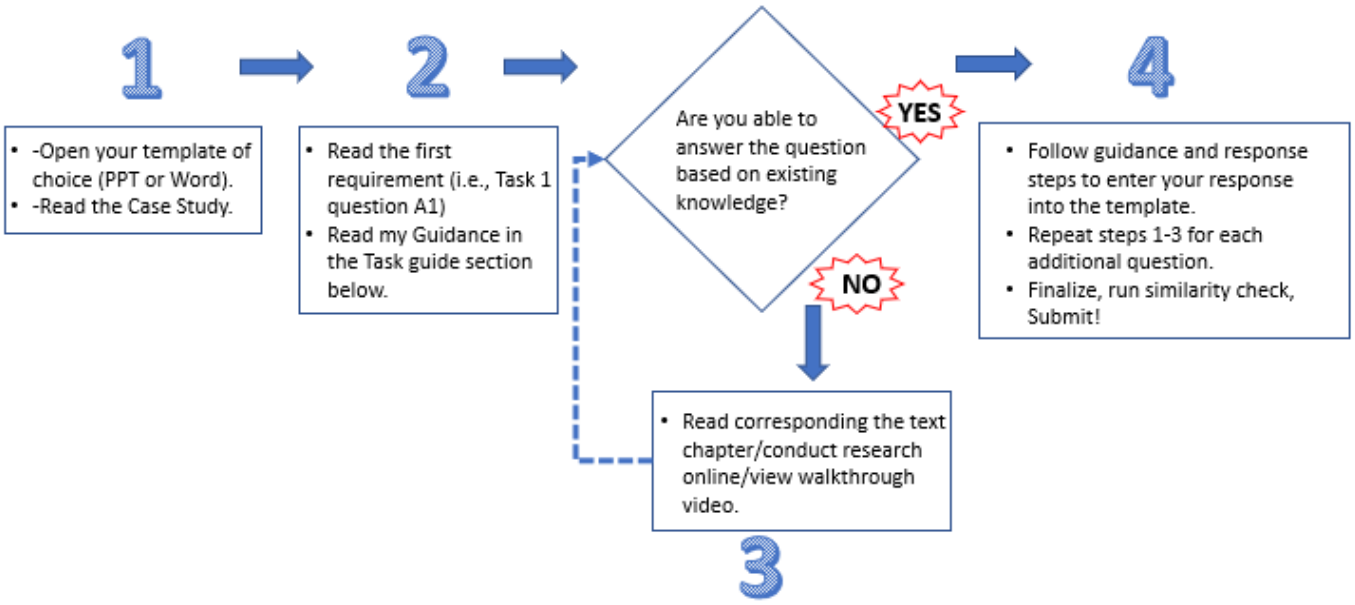
5. Be blatant and alleviate guesswork/interpretation for your evaluator. Don't assume the person reading your work can read your mind. Provide clarity in your responses by restating key parts of the questions in your responses.

6. Check spelling and grammar. Be sure to run spell check and proofread your work before submitting to avoid a task return for professional communication.

7. Run your similarity check. Be sure to run your similarity check and adjust your work to meet similarity requirements before submitting your work. Submitting work that doesn't meet similarity results in an automatic task return with no feedback on content as no evaluation will be conducted.

8. **Leverage your Assigned Course Instructor.** They are here to help you. Don't hesitate to email or schedule an appointment with your instructor if you have a question or run into a roadblock with your tasks. You can also sign up for the course cohort by clicking the "Explore Course Cohorts" button on your course page or view cohort recordings in the course tips section.

9. Recommended Approach:



Task 1 Guide

Requirement	Guidance	Response Steps
Task 1 A1. Explain how CFAA and ECPA each specifically relate to the criminal activity described in the case study. Chapters: 2, 12, 15	**CFAA** - Identify an instance of **intentional access to information on any of TechFite's computers without authorization.** TechFite computers are **protected computers** due to connectivity to the Internet for their business transactions. The Internet is an instrument of interstate commerce. **ECPA –** Identify an instance of **unauthorized access, use, disclosure, or interception of electronic communications.** Discussion of any one (access/use/disclosure/interception) will suffice. The electronic communications can also be stored or in transit.	1. **(CFAA)** Discuss a specific instance of criminal activity from the case study where information on a protected computer was accessed without authorization. 2. **(ECPA)** Discuss a specific instance of criminal activity from the case study where electronic communications were accessed, used, disclosed, or intercepted without authorization.

Requirement	Guidance	Response Steps
Task 1 A2. Explain how three laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study. Chapters: 2, 7, 12, 14, 15	You will need to provide three separate examples here. For each example you will **discuss a specific negligent** act that led to/contributed to a **specific violation of a specific law, regulation, or legal case**. You may use the three laws discussed in the task (SOX, ECPA, CFAA). **Negligence:** The best way to approach identifying negligent acts is to focus on intent and harm. Negligent acts are those that were done **unintentionally** and/or as a result of **carelessness**, but still has potential to or actually does **result in some form of harm**. **Justification of Legal Action**: Discussion of the **specific act violating** one of the three **laws** you select covers this part.	1. Discuss a specific instance of negligence observed in the case study that led to a violation of a specific law/regulation/legal case and justifies legal action. Discuss the specific law violated. 2. Repeat for the second and third required examples.

Requirement	Guidance	Response Steps
Task 1 A3. Discuss two instances in which duty of due care was lacking. Chapter 12	As you look for examples within the case study, think about instances where a person did not take action(s) they were reasonably expected to take which subsequently directly or indirectly led to unwanted occurrences in the case study. You need to provide two distinct examples.	1. Discuss a specific instance where someone failed to take a reasonably expected action and the negative outcome it led to or could potentially lead to. 2. Repeat for the second required example.

Requirement	Guidance	Response Steps
Task1 A4. Describe how the Sarbanes-Oxley Act (SOX) applies to the case study. Chapters: 7, 14	Think about how SOX applies to the company with respect to activities observed that constitute violations of the act. i.e. was there any activity that occurred that would illegally exaggerate the company's appeal to persuade investors or to create a possible avenue for embezzlement? What is SOX's stance on auditing as compared to TechFite's auditing policies, practices, or lack thereof? Keyword search financial within the case study.	1. Discuss a specific relation of the company to SOX. This can be by providing evidence of whether TechFite has to comply with SOX, and/or evidence of activity observed where the company actually violated SOX.

Requirement	Guidance	Response Steps
Task 1 B1/B1a. Identify who committed the alleged criminal acts and who were the victims. (Sufficient "evidence" provided in B1a and B1b covers B1) Chapters: N/A Elaborate on criminal activity discussed in part A	"*Who*" here actually means listing the specific persons or entities you feel committed the acts *AND* the persons or entities victimized by those actors/culprits. Ensure you have two or more distinct Actor/Act/Victim combinations to serve as your examples. For this section, if you want to focus on the criminal activity you discuss in a previous section, that is fine. You will however just need to (1) restate the crimes committed, and (2) actually provide the names of the culprits and victims.	1. Discuss a specific criminal act observed in the case study and explicitly list name the person/entity that committed the act and explicitly name the person/entity that was victimized by the act. 2. Repeat for the second required example using a **different actor, act and victim from the first example.**

Requirement	Guidance	Response Steps
Task 1 B1b. Explain how existing cybersecurity policies and procedures failed to prevent the alleged criminal activity. Chapter 13	Think about policies or procedures that either (1) were **in place at the company but ineffective**/not enforced, and/or (2) **that exist, but were not in place at the company;** that failed to prevent the criminal acts you identify. Cybersecurity policies and procedures include but are not limited to DLP policy, Chinese Wall policy, Auditing policy, separation of duties policy, account creation/termination policy, AUP, the list goes on... Discuss specific procedures that augment your selected policies, or that can stand alone to address specific issues. Note that each example above actually includes the word "policy" be sure yours do too.	1. Discuss a specific instance of criminal activity from the case study and a specific cybersecurity policy and corresponding procedure that could help prevent that activity. Include the name of the law or regulation the activity violates. 2. Repeat for the second required example.

Requirement	Guidance	Response Steps
Task 1 B2/B2a. Identify who was negligent and who were the victims. (Sufficient "evidence" provided in B2a and B2b covers B2) Chapter 12	"Who" here means actually listing the specific persons or entities you feel were negligent AND the persons or entities victimized. Ensure you have two or more Actor/Act/Victim combinations to serve as your examples. For B2a and B2b, you'll apply the same approach as you will for B1a and B1b, but with emphasis on the **negligent activity**. For B2b, it is fine to discuss the same cybersecurity policies and procedures you discuss for the criminal activity if they will also address the negligent activity. Just be sure to articulate how.	1. Discuss a specific negligent act observed in the case study and explicitly list name the person/entity that committed the act and explicitly name the person/entity that was victimized by the act. 2. Repeat for the second required example using a **different actor, act and victim from the first example.**

Requirement	Guidance	Response Steps
Task 1 B2b. Explain how existing cybersecurity policies and procedures failed to prevent the negligent practices. Chapter 13	Think about policies that either (1) were in place at the company and not enforced/ineffective, and/or (2) policies that exist, but were not in place at the company; that failed to prevent the **negligent activity** you identify. Cybersecurity policies and procedures include but are not limited to DLP Policy, Chinese Wall Policy, Auditing policy, separation of duties, account creation policy, AUP, the list goes on...	**1.** Discuss a specific instance of negligent activity from the case study and a specific cybersecurity policy and corresponding procedure that could help prevent that activity. **2.** Repeat for the second required example.

Requirement	Guidance	Response Steps
Task 1 C. **Summarize the status of TechFite's legal compliance for its senior management.** Chapter: 3	You will simply list each law/regulation/legal case you discuss in parts A&B, and explicitly state whether the company was compliant with each and why. Complete in a paragraph or two.	• State the Law • State TechFite's Compliance Status (compliant or not compliant) • Discuss why the company is non-compliant in more detail. Repeat for **each law discussed in parts A and B**.

Task 2 Guide

Requirement	Guidance	Response Steps
Task 2 A1/A1a. Discuss the ethical guidelines or standards relating to information security that should apply to the case study. Justify your reasoning. Chapter: 13	Note that "guidelines/"standards" in the requirements is plural. Be sure to identify and discuss at least two different guidelines/standards. Actually (literally) call your selected guidelines, "guidelines". i.e. "An ethical guideline related to information security used by GIAC states [insert guideline here]." OR "An ethical guideline related to information security states [insert guideline here]." Mention of the organization from which you pulled your guideline or standard from is not required. Leverage the "Ethical Guidelines Help" section below!!!	**1.** Identify an organization **2.** Locate the organization's code of ethics. **3.** From the organization's code of ethics, identify an entry (entries in the organization's code of ethics are the standards/guidelines) related to information security and related to a specific activity from the case study. **4.** Discuss how the selected standard/guideline relates to the case study example and could help prevent the activity if adopted by TechFite. **5.** Repeat steps 1-4 to provide the second required ethical guideline discussion.

Requirement	Guidance	Response Steps
Task 2 A2. Identify the behaviors, or omission of behaviors, of the people who fostered the unethical practices. Chapter: N/A. Use the guidance in this document, and your judgement.	"*…of the people*" here means actually discussing behaviors/omissions of behaviors of specific individuals. Also note that "*people*", "*behaviors*" and "*practices*" in the requirements are all plural, so ensure you discuss at a minimum total for the section, two or more people, two or more behaviors, and two or more practices.	**1.** Identify a specific person that did something or failed to do something that fostered unethical practices by others. **2.** Repeat step 1 with a second example.

Requirement	Guidance	Response Steps
Task 2 A3. Discuss what factors at TechFite led to lax ethical behavior. Chapter: N/A. Use the guidance in this document, and your judgement.	Think cause and effect here, i.e. tie the factors to the resulting behavior to justify your reasoning.	**1**. Identify and discuss a specific factor (this can be a condition, observed activity, company posture etc.) that set the tone that acting ethically was not important. Discuss specific behavior that resulted. **2.** Repeat step 1 with the second required example.
Requirement	**Guidance**	**Response Steps**
Task 2 B1. Describe two information security policies that may have prevented or reduced the criminal activity, deterred the negligent acts, and decreased the threats to intellectual property. Chapter: 10, 13	This section calls for you to discuss two specific information security policies. Be sure to articulate how your selected policies tie to the criminal activity you identified ***AND*** to the negligent activity you identified ***AND*** to intellectual property in the manner specified in the requirements. This question may sound very familiar to Task 1 B1b and B2b to you unless you are working on the tasks out of order and started with task 2 first. There is subtle rewording and the addition of threat to intellectual property. So essentially, you will likely be able to grab from those sections in task 1 and tie in the intellectual property threat relevance.	1. Follow general steps you used in B1b/B2b, but specifically tie in how threat to intellectual property would be addressed. 2. Repeat for your second required example.

Requirement	Guidance	Response Steps
Task 2 B2. Describe the key components of a Security Awareness Training and Education (SATE) program that could be implemented at TechFite Chapter: 13	*"Components"* here include: 1-Who will oversee/manage the program 2-Who will be required to participate (take/receive training) 3-Who will deliver the training 4-What the repercussions for non-compliance are. Listen here: SATE Components	1. Discuss one of the four "components" (from the list in the general guidance column) of your recommended SATE program. 2. Repeat using a different component for your second required example.

Requirement	Guidance	Response Steps
Task 2 B2a. Explain how the SATE program will be communicated to TechFite employees. Chapter: 13	This section is asking how the program will "communicated", not for further elaboration on "what" SATE is. Imagine you were responsible for introducing this newly developed SATE program to the company staff, how would you go about accomplishing that? Via email?, verbally to each employee via Styrofoam cup & string phones?	1. Explicitly state the mechanism that will be used to inform the TechFite staff they now have a SATE program.

Requirement	Guidance	Response Steps
Task 2 B2b. Justify the SATE program's relevance to mitigating the undesirable behaviors at TechFite. Chapter: 13	For this section, you will be more or less selling the idea of implementing a SATE program. Select a minimum of two specific undesirable behaviors from the case study and explain how the SATE program will help mitigate them. For instance, let's say you encountered an attack at your organization and one of the factors that contributed to the success of the attack was an employee being manipulated to do something during a social interaction with someone. Inclusion of periodic social engineering training into the SATE program would help mitigate that particular behavior.	1. Identify and discuss a specific undesirable behavior from the case study. 2. Discuss training or education aspect that will be included in your recommended SATE program that would mitigate the identified behavior and thereby benefit TechFite. 3. Repeat steps 1&2 for your second required example.
Requirement	**Guidance**	**Response Steps**
Task 2 C. **Summarize TechFite's ethical challenges and the related mitigation strategies from part B for its senior management.**	You will simply restate each ethical challenge you observed from the case study and discussed in parts A and B along with the recommended mitigation strategies for each. Complete with a paragraph or two	• Restate a specific ethical issue from discussion in parts A and B. • Discuss the mitigation for the issue. Repeat for each issue discussed in parts A and B.

Ethical Guidelines Help

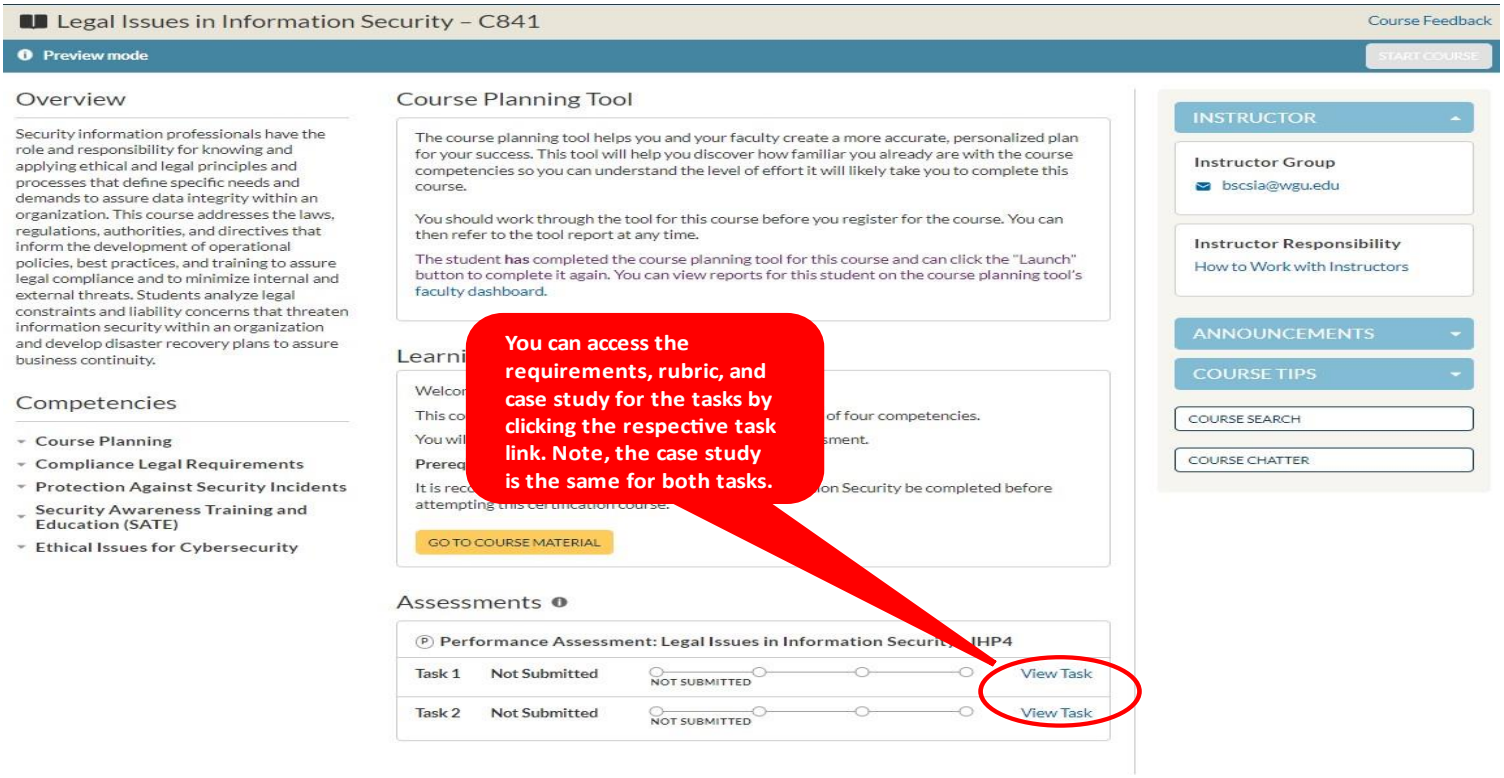
Organization/Source	Ethical Guideline Related to Information Security
EC Council - https://www.eccouncil.org/code-of-ethics/	Keep private and confidential information gained in your professional work, (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.
EC Council - https://www.eccouncil.org/code-of-ethics/	Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
EC Council - https://www.eccouncil.org/code-of-ethics/	Neither associate with malicious hackers nor engage in any malicious activities.
EC Council - https://www.eccouncil.org/code-of-ethics/	Ensure all penetration testing activities are authorized and within legal limits.
EC Council - https://www.eccouncil.org/code-of-ethics/	Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
ISSA - https://www.issa.org/code-of-ethics/	Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities; Discharge professional responsibilities with diligence and honesty.
ISSA - https://www.issa.org/code-of-ethics/	To promote practices that will ensure the confidentiality, integrity, and availability of organizational information resources, professionals should: Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles
ISSA - https://www.issa.org/code-of-ethics/	Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of or is detrimental to employers, the information security profession.
ISSA - https://www.issa.org/code-of-ethics/	Promote generally accepted information security current best practices and standards.
GIAC - https://www.giac.org/policies/ethics/	Not to engage in or be a party to unethical or unlawful acts that negatively affect the community, my professional reputation, or the information security discipline.
GIAC - https://www.giac.org/policies/ethics/	Not to share, disseminate, or otherwise distribute confidential or proprietary information pertaining to the GIAC certification process.
GIAC - https://www.giac.org/policies/ethics/	Protect confidential and proprietary information with which I come into contact.
GIAC - https://www.giac.org/policies/ethics/	Minimize risks to the confidentiality, integrity, or availability of an information technology solution, consistent with risk management practice.

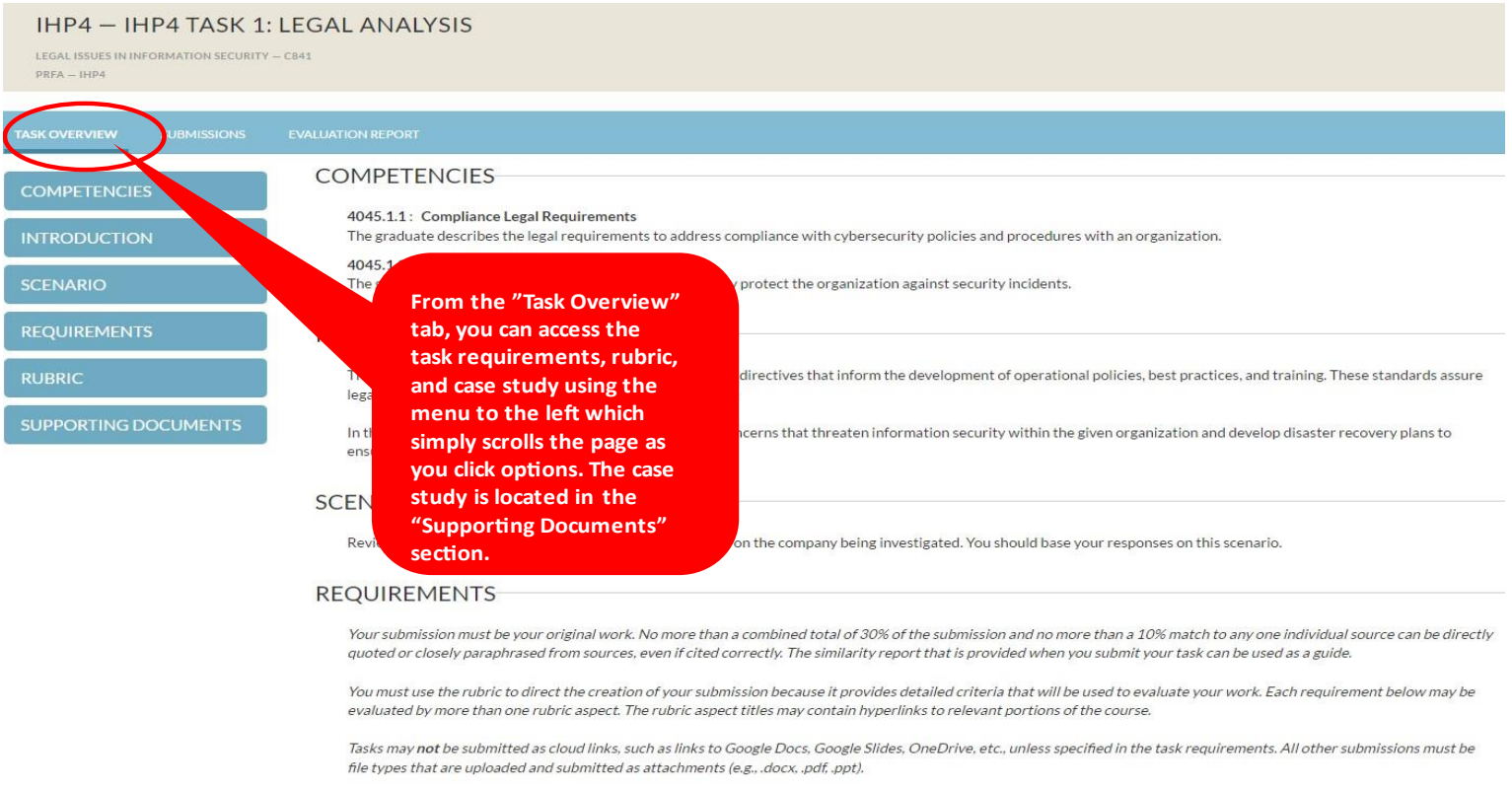
GIAC - https://www.giac.org/policies/ethics/	Not to misuse any information or privileges I am afforded as part of my responsibilities.
ASIS - https://www.asisonline.org/globalassets/membership/documents/asis-code-of-ethics.pdf	Due care requires that the professional must not knowingly reveal confidential information or use a confidence to the disadvantage of the principal or to the advantage of the member or a third person unless the principal consents after full disclosure of all the facts. This confidentiality continues after the business relationship between the member and his principal has terminated.
ASIS - https://www.asisonline.org/globalassets/membership/documents/asis-code-of-ethics.pdf	A member shall not disclose confidential information for personal gain without appropriate authorization.
ASIS - https://www.asisonline.org/globalassets/membership/documents/asis-code-of-ethics.pdf	A member shall safeguard confidential information and exercise due care to prevent its improper disclosure.
ISC2 - https://www.isc2.org/Ethics	InfoSec Professionals should: Act honorably, honestly, justly, responsibly, and legally.
ISC2 - https://www.isc2.org/Ethics	InfoSec Professionals should: Protect society, the common good, necessary public trust and confidence, and the infrastructure.
ACM - https://www.acm.org/code-of-ethics	Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups.
ACM - https://www.acm.org/code-of-ethics	Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, or organizational regulations.
CSA - https://cloudsecurityalliance.org/artifacts/code-of-ethics/	Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of activities.
CSA - https://cloudsecurityalliance.org/artifacts/code-of-ethics/	Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of or is detrimental to employers, or the information security profession.
ISACA - https://www.isaca.org/credentialing/code-of-professional-ethics	Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
ISACA - https://www.isaca.org/credentialing/code-of-professional-ethics	Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security and risk management.

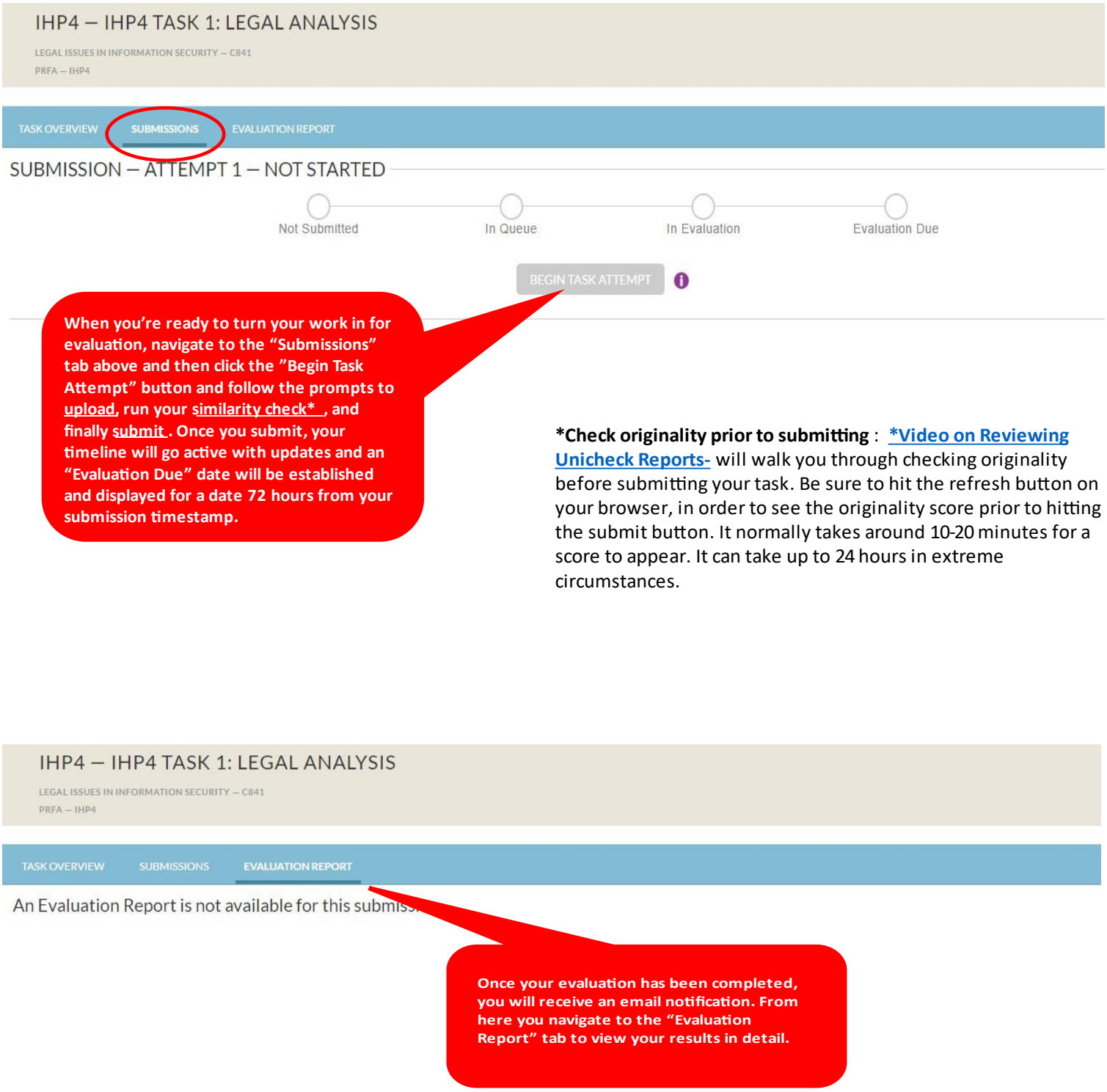
Pacing Help

		Nine key lessons I have found are most helpful for completing the course task are Lessons 1, 2, 3, 7, 10, 12, 13, 14, and 15. This coupled with guidance within the task guidance make for a focused and efficient approach to ensure you complete the course. Work through the steps for each task, using the lesson readings as needed to fill knowledge gaps. Fit the steps into your completion timeline) or goal (i.e., adjust up or down from the 2-week timeframe to fit your plans and hold yourself accountable for completing steps on time.
	Two-Week Pacing Plan	
		Task 1
	Day 1-3	**(1)** Read Chapters 1, 2, 12, 15 > Leverage the task guidance spreadsheet to complete Task Section A1, and ECPA & CFAA portion of Task Section A2
	Day 4-5	**(2)** Review Negligence Torts section of Chapter 12 > Leverage the task guidance to complete Task Section A3 **(3)** Read Chapters 7 and 14 > Leverage the task guidance to complete the SOX portion of Task Section A4
	Day 6	**(4)** Revisit Chapters 2, 7, 13, 15 as needed > Leverage the task guidance to complete Task Section B1a **(6)** Read Chapter 13 > Leverage the task guidance to complete Task Section B1b
	Day 7	**(5)** Review Negligence Torts section of Chapter 12 > Leverage the task guidance to complete Task Section B2a **(6)** Revisit Chapter 13 as needed > Leverage the task guidance to complete Task Section B2b
	Day 8	**(7)** Read Chapter 3 > Leverage the task guidance to complete Task Section C **Submission**: View similarity check video and adjust similarity > Submit!
		Task 2
	Day 9	**(1)** Review Chapters 13 if/as needed. > Leverage the task guidance to complete Task Section A1a
	Day 10	**(2)** Leverage the task guidance to complete Task Section A2 **(3)** Leverage the task guidance spreadsheet to complete Task Section A3
	Day 11	**(4)** Read Lesson 10. Review lesson 13 if/as needed. > Leverage the task guidance to complete Task Section B1
	Day 12	**(5)** Review Chapter 13 if/as needed. > Leverage the task guidance to complete Task Section B2, B2a, and B2b
	Day 13	**(6)** Review Lesson 3 if/as needed> Leverage the task guidance to complete Task Section C within **Submission:** View similarity check video and adjust similarity > Submit!

Submitting Your Tasks







***Check originality prior to submitting** : ***Video on Reviewing Unicheck Reports-** will walk you through checking originality before submitting your task. Be sure to hit the refresh button on your browser, in order to see the originality score prior to hitting the submit button. It normally takes around 10-20 minutes for a score to appear. It can take up to 24 hours in extreme circumstances.