Step 1: All four projects for this course will be completed from the vantage point of a specific industry and an organization assigned to you by the instructor. If you do not know your assigned organization, contact your instructor immediately. If you want to use another organization than the one assigned you or one not listed, contact your instructor as well.

Familiarize yourself with the organization and breach your instructor has assigned by reviewing the details at <https://www.databreaches.net/>. The descriptions include an overview and key information about the organization on the internet, as well as information about a breach or attempted breach. For the purposes of this course, you will assume this organization is your employer.

You may wish to briefly research your assigned organization to gather additional information about the organization and its security posture.

Step 2: Write a Cybersecurity Background Summary

In Step 1, you familiarized yourself with your assigned organization. Now, it is time to write a cybersecurity overview. Write a three-page background summary that includes a general overview of cybersecurity and a section on enterprise cybersecurity.

Include the following items in the general overview of cybersecurity:

* Compare and contrast cybersecurity and computer security.
* Discuss [data flows across networks](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/data-flows-across-networks.html?ou=622377). As part of this discussion, it may help to review the following topics: [binary digits](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/binary-digits.html?ou=622377), [nontextual data](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/nontextual.html?ou=622377" \t "_blank), [ASCII](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/american-standard-code-for-information-interchange.html?ou=622377), [hexadecimal](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/hexadecimal.html?ou=622377), [computer networks](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/computer-networks-introduction.html?ou=622377), [network devices and cables](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/network-devices-and-cables.html?ou=622377), and [network protocols](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/network-protocols.html?ou=622377).
* Discuss basic cybersecurity concepts and vulnerabilities, including flaws that can exist in software. As part of this discussion, it may help to review the following topics: [systems, utilities, and application software](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/systems--utilities--and-applications-software.html?ou=622377), [software](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/software.html?ou=622377), [interaction of software](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/interaction-of-software.html?ou=622377), and [creating a program](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/creating-a-program.html?ou=622377).
* Discuss common cybersecurity attacks. Helpful topics include [protocols, web sessions, and security issues](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/protocols--web-sessions--and-security-issues.html?ou=622377), [servers and firewalls](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/servers-and-firewalls.html?ou=622377), [a closer look at the World Wide Web](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/closer-look-at-the-web.html?ou=622377) and [web markup language](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/web-markup-languages.html?ou=622377), [cyberattacks](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/cyberattacks.html?ou=622377), and [attack vectors](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/attack-vectors.html?ou=622377).
* Discuss [penetration testing](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/penetration-testing.html?ou=622377).
* Discuss how to employ [network forensic analysis tools (NFAT)](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/network-forensics.html?ou=622377) to identify software communications vulnerabilities.

Include the following items in the enterprise cybersecurity section:

* List and discuss the major concepts of enterprise cybersecurity, including [confidentiality, integrity, and availability](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/confidentiality--integrity--and-availability.html?ou=622377) (CIA)
* Discuss the principles that underlie the development of an enterprise cybersecurity policy framework and implementation plan.
* List the major types of cybersecurity threats that a modern enterprise might face.

You will attach this cybersecurity background summary to the security assessment in a later project step.

Submit the cybersecurity background summary for feedback.

Step 3: Analyze Security Weaknesses

After writing the cybersecurity background summary, you are ready to analyze the security weaknesses of your assigned organization. When analyzing cybersecurity weaknesses, there are several areas to consider.

Analyze the organization’s security from the following perspectives:

1. a technology perspective
2. a people perspective
3. a policy perspective

You will include this information in the security assessment. In the next step, you will consider risk factors.

Step 4: Compile a Risk Summary

Now that you have looked at security weaknesses, it’s time to identify areas that should be improved or strengthened, including potential risks associated with maintaining the current security posture. Discuss how you would employ network analysis tools to identify software communications vulnerabilities. Make sure to include the following information:

1. Classify risks according to relevant criteria.
2. Explain system and application security threats and vulnerabilities.
3. Prioritize risks from internal and external sources.
4. Assess the cybersecurity threats faced by your entity.

You will include this information in the security assessment, which you will compile in the next step.

# Step 5: Submit a Security Weakness Assessment

From the information that you gathered in the previous steps, develop a two-page summary of your organization’s security weaknesses. Identify threats, risks, and vulnerabilities to achieve a holistic view of risk across the entity.

Consider areas that should be improved from a technology perspective, a people perspective, and a policy perspective. Also note potential risks associated with maintaining the current security posture. You will reference this security assessment later when you make your business case and final recommendation.

Submit the security assessment for feedback.

Step 6: Begin a Security Models Summary

[Confidentiality, integrity, and availability](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/confidentiality--integrity--and-availability.html?ou=622377) (CIA triad), as well as authentication and nonrepudiation, are fundamental security concepts that must be considered when assessing and developing security options. [Cybersecurity models](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/cybersecurity-models.html?ou=622377) have been developed to address some or all of these security concepts.

While these models were generally created to address a specific business case, each of the models has attributes that could be used to assemble a custom security plan. In order to draft a custom security plan for your organization, you will need to understand basic security models. You will identify key features, weaknesses, and targeted sectors and/or infrastructures.

In this step and the following step, you will develop a short summary for each of the security models listed. These reports will serve as an Appendix A to the final memo and will document the security models and their attributes in advance of the memo that you will deliver with your recommended approach.

Each summary should include a descriptive and evaluative paragraph on the following attributes:

Include the origins of the model (who developed it, when was it developed, and the context under which it was developed), main characteristics of the model (details on the business, sector, industry for whom the model was developed), and key features of the model.

Write summaries for the following common models:

* Bell-LaPadula
* Biba’s Strict Integrity Policy
* Clark-Wilson
* Chinese Wall

When you have completed these summaries, continue to the next step, where you'll write a summary for the next four security models.

Step 7: Continue the Security Models Summary

Continue summarizing the various c[ybersecurity models](https://leocontent.umgc.edu/content/scor/uncurated/cmp/2218-cmp610/learning-topic-list/cybersecurity-models.html?ou=622377), as in the previous step. Again, identify key features, weaknesses, and targeted sectors/infrastructures and develop a short summary for each of the security models listed below. These reports will be added to Appendix A for the final memo and will document the security models and their attributes in advance of the memo that you will deliver with your recommended approach.

Each summary should include a descriptive and evaluative paragraph on the following attributes:

Include the origins of the model (who developed it, when was it developed, and the context under which it was developed), main characteristics of the model (details on the business, sector, industry for whom the model was developed), and key features of the model. Write summaries for the following models:

* Clinical Information Systems Security
* Noninterference Security
* Deducibility Security
* Graham-Denning

When you have finished both steps and the Security Models Summary, submit Appendix A for feedback.

# Step 8: Analyze the Security Models

Now that you are familiar with existing common security models, analyze each of the security models that you reviewed in the last two steps and their attributes against the needs of your organization as identified in the earlier steps. The information that you gather here will contribute to your security plan.

In the next step, you will look at features that will work for the organization.

# Step 9: Identify Relevant Model Features

Next, identify features from the models that apply to your assigned organization’s security needs. Also include any security attributes that you believe are important for your organization but are not included in any of the models. The information that you gather here, along with the information gathered in the previous step, will contribute to the security plan.

When you are finished, in the next step you will put together a security plan for the organization.

Step 10: Design a Custom Security Plan

Having completed an assessment of your organization’s security posture and the analysis of security models, you will now design a custom security plan for the organization. The custom security plan should meet the following criteria:

* The security plan should coincide with the organization's IT vision, mission, and goals.
* Include an information security program that aligns with business strategy.
* Incorporate all internal and external business functions within the organization's security programs.
* Classify risks according to relevant criteria.
* Prioritize threats from both internal and external sources.
* Rank the most relevant security attributes for the organization and list them in priority order. This list will serve as Appendix B to your final assignment.

Submit Appendix B for feedback.

# Step 11: Develop a Business Case for Your Organization

With the new security plan written, you will need to develop a business case for it to include in the memo to the CTO. Using your knowledge of the organization’s security posture from Step 1 and your understanding of applicable security model features, make the case for changes to the organization. Include the rationale for change and any impacts to the business.

Also include an implementation plan. Describe the present situation in the organization and the associated risks assumed given the security weaknesses.

The work you do in this step will become the first of three sections of the three-page memo in the last step of the project.

In the next step, you will work on another section of the memo, security models.

# Step 12: Identify Security Model Attributes

Next, detail the security model attributes that best apply to the organization. Identify the model, if any, from which the attributes are derived and why the attribute applies to the organization.

The work you do in this step will become the second section of the memo in Step 14.

In the next step, you will look at how security in the organization could be improved, based on your recommendations.

# Step 13: Assess Security Improvement Potential

Finally, give your best judgment on the potential to improve the security posture of the organization when your recommendations are implemented. You will need to evaluate the pros and cons of implementation in relation to CIA. Discuss the risks and impacts to include a high-level assessment of financials. Consider how business continuity and continued alignment will be maintained.

The work you do in this step will become the third section of the memo in the final step.

Step 14: Develop and Submit a Security Plan Recommendation Memorandum

Compile the analyses completed in the last three steps into a memorandum from you to your supervisor. This memo should be three pages, excluding Appendices A and B, and should clearly articulate the business case for adopting features from the reviewed security models. It should include the following:

* a description of the security model attributes
* an assessment of the weaknesses in the organization that the security features will address
* your rationale for selecting the specific security attributes and your prognosis of success, noting risks and impacts to include a high-level assessment of financials
* the policies and procedures that will need to be in place for the security plan to work
* the infrastructure that will need to be in place for the security program to operate and to align with each entity within the organization
* a plan for evaluating the security plan's effectiveness

Update the appendices according to the feedback received. Submit the memorandum along with Appendices A and B.