Pls do no not plagiarize it will be turn in into trunitin and make sure you look and use the document in the download. Strategic Cybersecurity Management Experimental Learning Assignment Creating a Custom Strategic Cybersecurity Plan Risk Management Assignment Overview Cybersecurity is all about managing risk. Risk cannot be totally eliminated in most cases but you need to understand your internal environment and the various threats against it. Then you need to take the necessary steps to mitigate or control them based on the risk appetite of the company. In the class session and with the learning activities you have learned a great deal about Risk Management, Risk Analysis, Risk Identification, and Risk Controls (NIST documents). This is an opportunity for you as the CISO to practice your Risk Management skills. This is a “hands-on” experiential learning experience. In this assignment, you will be identifying and describing assets, vulnerabilities and mitigation strategies. Select (5) information assets from your company inventory that you feel are important to the success of your company. Provide a high level description of each information asset and then briefly explain why each of these information assets is important. An information asset can be just about anything that is important to your company such as: • Hardware: ex. Your company’s web server • Software: ex. A new mobile app • Company Information: ex. Your product’s secret recipe • Customer Data: ex. Customer’s credit card numbers, PII, others For each of the (5) identified assets, determine its appropriate classification category and corresponding value to the profitability of the company. You must also include an explanation of your classification scheme and how you are determining the profit value so your audience understands your reasoning. Use visual elements to display your information. A portion of your grade will be based on how you communicate your information. For each Asset, select (1) vulnerability that you believe is most worrisome for that particular Asset. Provide a high level description of the vulnerability and then briefly explain why you chose it. You should have a total of (5) vulnerabilities when this part of the analysis is complete: 1 vulnerability per asset. For each of the (5) identified vulnerabilities, determine their corresponding probability and impact consequence. You decide how to represent the probability and impact consequence but you must also include an explanation of your decision process so your audience understands your reasoning. Use visual elements to display your information. You can use a numerical score, a color scheme or even High/Medium/Low type system. A portion of your grade will be based on how you communicate your information. 1 Finally, determine the appropriate risk mitigation strategy and the appropriate security controls for each of the (5) identified vulnerabilities. You must also include an explanation of your controls and why they are the best choice for the particular vulnerability. Most risks will require more than a single control to mitigate them. Your 5 assets, 5 vulnerabilities, 5+ controls (recommendations) should be listed in a table. Remember CIA and data classification are important. Additionally, likelihood of occurrence is a good way to highlight critical and high risk items in an effort to prioritize and focus the executives attention and budget priorities. Once your tables(s) are created they are also a good way to summarize your risk report and ask for their permission to move forward with the recommended plans.

Finally, determine the appropriate risk mitigation strategy and the appropriate security controls for each of the (5) identified vulnerabilities. You must also include an explanation of your controls and why they are the best choice for the particular vulnerability. Most risks will require more than a single control to mitigate them. Your 5 assets, 5 vulnerabilities, 5+ controls (recommendations) should be listed in a table. Remember CIA and data classification are important. Additionally, likelihood of occurrence is a good way to highlight critical and high risk items in an effort to prioritize and focus the executives attention and budget priorities. Once your tables(s) are created they are also a good way to summarize your risk report and ask for their permission to move forward with the recommended plans. Your assignment should be in a “Word” document (not .pdf) format to allow me to provide feedback within the document. Upload your Risk Project in the word file in the Risk information assignment box. Please be sure to name the word file document using the following naming convention to make it easier for everyone to manage: (ex: Blanke\_Risk) Grading Metrics – Risk Report 100 points 1. The Asset portion of this assignment will be worth (30 pts) 2. The Vulnerability portion of this assignment will be worth (30 pts) 3. The Mitigation portion of this assignment will be worth (20 pts) 4. Keep in mind that how well you visually represent all this information in an easy to understand format will be part of the grading criteria. You will not receive full credit if all you use is text to complete this assignment 5. Provide a Reference List and use APA formatting within your report. I should see that you are using at least 10 references for your report and your book plus a specific part of the lecture should be one of those references (20 pts) Grading Metrics – Risk Presentation – 50 points 1. Prepare 3-5 .ppt slides (30 points) 2. These should be professionally developed (10 points) 3. Each slide should have notes of what you are saying to the Executives (10 points) CYBS 8396 Strategic Cybersecurity Management Experimental Learning Assignment – Part 1 & Part 2 Creating a Custom Strategic Cybersecurity Plan One of the major deliverables for this course is to create a Strategic Cybersecurity Plan. This plan will be created in two parts (check your syllabus for the due dates). I strongly recommend that you build your Strategic Cybersecurity Plan each week as we progress through the Units. Do not wait until the Unit it is due to start writing your plan. There is also a presentation of the entire plan that is due at the end of the semester and it will be reviewed by your peers. The class sessions, learning activities, assignments, and discussions in each unit will provide key information that should be included in your plan. I am looking for your understanding of the work we have covered in the class sessions, assignments, learning activities, and discussions. Each of these learning components will provide you the baseline to create your company’s Strategic Cybersecurity Plan. You are expected to customize your plan and program for your specific company and tailor the plan to fit your organization. While many companies face similar external threats and vulnerabilities, they all have different cultures and levels of risk tolerance. Describing why various components are part of your plan is just as important as what you include. Your plan must contain all of the components described in this document at a minimum but you are free to add additional items that are important to your Strategic Cybersecurity Plan. You should also conduct your own, independent research on the various topics to help you develop your Strategic Cybersecurity Plan. This is not a cut and paste assignment. This is a creative assignment where you create your business and the Strategic Cybersecurity Plan that fits your business and addresses the specific challenges of your environment. Valuable creativity with well thought out justifications and insightful additions will be recognized and may be awarded extra points at the discretion of the Professor. Review this document carefully and follow the instructions. A high level outline showing the major components of each part of the paper is provided along with the total points possible for that section. It is followed by a detailed explanation of what is expected in each section. The detailed requirements are organized roughly by class units where possible. Let me say again, I strongly urge you to build your Strategic Cybersecurity Plan each and every week as we progress through the Units. Do not wait until the Unit it is due to start writing your plan. Again, your Strategic Cybersecurity Plan will be composed of 2 separate papers: Part 1 and Part 2. Check your syllabus for the due dates. Please contact me if you have any que

The placement of the security team within an organization impacts not only its performance but also its relationship with other departments. Visually create an organization chart for your Cybersecurity team. Think about what you learned from the NICE structure and the text book when creating your org-chart. The org-chart must at least show the following: • Placement within the organizational hierarchy. • Reporting structure and security position titles. • Number of dedicated security employees. • Employees in other departments who have specific security duties. • Highlight any special security resources such as consultants or contractors. Again, these particular items must be addressed in your org-chart but you are free to include other aspects if you feel they are appropriate for your situation. Describe your security organization by listing the various security roles and high level security responsibilities of the security team members. Be sure to include and explain any Cybersecurity specific responsibilities that you are expecting other departments in the company to own and carry out. Rarely does the security team perform all security activities. For instance, in many companies the Help Desk Support Group is responsible for helping users reset their forgotten passwords. Now you must justify your org-chart. Explain why you chose this particular reporting structure and the various security roles. Do you have enough resources or too many? Do you have any open positions now or in the future? Explain why this is the best organizational structure for your company, Cybersecurity team and business environment. Finally, draft a Security Mission statement that aligns with the Business and IT. The next step is to identify and describe (5) security core values that are important to your organization as you create your own security culture. These core values must enhance and support your Cybersecurity program. Explain the significance and relevance of each of these core values to your Cybersecurity program, don’t just list them and also explain how they align with the business. Finally, identify and describe (5) strategic Cybersecurity issues or challenges that your company is facing now or will face in the near future. A number of issues were discussed during the semester so far but you are free to add any strategic Cybersecurity issue that you feel is important and relevant. Describe at a high-level how each of these issues and challenges effect your organization and why they must be addressed. Paper Mechanics: I expect the paper and presentation are formatted including proper spelling and grammar. Please include a title page and table of contents. Use various techniques to make your paper easy to read and understand. Include diagrams, tables, lists, charts, graphs, pictures and other features to make it look professional. I will deduct points for papers that contain only text. Be sure to explain industry specific acronyms and terminology for your audience. Finally, properly cite all reference materials. You must include external references in your paper to get full credit. Using references will add credibility to your plan.