CYBR3030 – Portfolio Assignment

**Course mark weighting:** 35%

**Objectives**

* Paraphrase concepts, skills and issues and describe how processes of authentication, authorization and accountability directly relate to the cybersecurity industry

**Purpose:**

This portfolio will be produced as a partial requirement to the course learning outcomes of CYBR 3030, Identity Management. The main objective for completing this assignment is to support your skills in evaluating authentication, authorization, and accountability in cybersecurity. This assignment will provide you with new perspectives that will support your critical thinking skills in the field which is beneficial for your career.

In addition, developing a portfolio will make your learning experience more direct as you translate your workplace and personal experiences into documented evidence. You can then learn to critically examine the nature of your learning and demonstrate your analytical skills in a comprehensive manner. Finally, this will give you the opportunity to enhance your analysis and written communication skills which are deemed crucial for cybersecurity professionals.

**Structure/Content of Portfolio:** Maximum 18 pages excluding your references. 12pt font, double spaced.

* Cover page (One page)
  + Course name and code
  + Student name and ID
  + Instructor Name
* Table of Contents (One page)
  + Headings and associated page numbers
* Introduction (One Page)
  + A brief introduction of your portfolio and any special structure in your document that your readers must know before proceeding with the rest of the content.
* A **self-reflection**, **critical review**, and **addition comments** for each of the required topics.
* References used in your critical review.

Required Topics:

* IAM Fundamentals
  + 1.0 Foundations of Identity & Access Management (IAM)
  + 2.0 Authentication Mechanism & management
  + 3.0 Authorization & Accountability
  + 4.0 Managing IAAA in Windows
  + 5.0 Managing IAAA in Linux
* Enterprise IAM
  + 6.0 Enterprise Identity Repository
  + 7.0 Privileged Access Management
  + 8.0 Enterprise Password Policy Management
  + 9.0 Integrated Access Management & IDM
  + 10.0 Applying Access Management & IDM
  + 11.0 Network Authentication & Access Protocol
* IAM Governance
  + 12.0 Data Ownership & Access Validation
  + 13.0 Identity & Access Validation
  + 14.0 Segregation of Duties & Job Rotation

Here is some Q and A to clarify the requirements

* What is a **self-reflection**? (example on following page)
  + A summary of the concepts, skills, and issues discussed in that topic including all reading materials covered for that topic. This section will capture what you have learned.
* What is a **critical review**? (example on following page)
  + Discuss the pros/cons or your weekly reflection and the importance of that topic in the specific situation/settings/organization. This section will capture why is that topic important.
* What **additional comments** are required? (example on following page)
  + What specific concept, skill, or issue and discuss how the organization could benefit from it. For example, how could organization benefit from a specific implementation or a solution to an issue.
* Overall personal reflection/Final Thoughts (One page)
  + Final thoughts that goes beyond the topics covered in this course and discuss the importance of the topics in the field of cybersecurity.
* References
  + Outline all references used to complete your portfolio. You may use APA or IEEE format. You must have at least 1 external reference per topic (11 total) supporting your critical review. These must be beyond the course content, or references mentioned in the slides.
  + It is assumed that you all will be referring to course content, only passages or excerpts from the content must be cited over and above assumed knowledge gained from the course content.
* **Can I use AI to assist me in this assignment?**
  + As per NAIT’s academic standards any use of AI must be properly cited, and failure to do so will result in academic misconduct investigations.
  + For the purposes of this assignment, generative AI can be used to clarify your writing but not to generate your reflections.
    - If you choose to use generative AI to clarify your writing you must submit your draft assignment and/or prompts along with your final version.
    - **Failure to submit draft/prompts will result in a grade of 0 being assigned.**

**Submission**

* The document must be created using Microsoft Word and saved in .docx format. You are expected to submit all data via Brightspace
* The deadline for the submission is outlined in the course calendar **but is due 7 days after** the completion of *Topic 14.0 Segregation of roles & job rotation*.

**Examples:**

See Brightspace for an example   
   
The false topic used below is; Why IPV4 is superior to IPV6.

**Marking Guide**

A, B, and C applies to each topic.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Advanced (3) | Proficient (2) | Developing (1) | Not Demonstrated (0) |
| **Self-Reflection (A)** | The depth of self-reflection goes beyond basic understanding of the topic | Foundational understanding is demonstrated | An introduction understanding of the topic is reflected | No sufficient evidence of topic demonstration |
| **Critical Review (B)** | Can draw a relationship between pros/cons and how it ties to a specific case study/project in the industry | Articulate pros and cons. Highlights industry relevance | Identifies basic pros and cons with introductory understanding of industry relations | No evidence of pros and cons or industry relevance |
| **Additional Comments (C)** | Clearly articulate problem-solving solutions based on a specific CSI within a specific context in the industry | Identify specific CSI and draw a direct benefit to a problem-solving situation with without drawing association with the industry | Basic introduction to CSI with little problem-solving solutions and no associations to the industry | Evidence of CSIs is not demonstrated |
| **Format** | Included all sections (cover page, ToC, Introduction, topics, and references) and formatted consistently | Few missing sections (cover page, ToC, Introduction, topics, and references) and/or some format inconsistencies | Used a different format but did not justify in the introduction page | Did not include required sections or use a format |
| **Language** | Language is professional, direct, and relevant to the topic. No grammar or spelling errors | Language is professional, direct, and relevant to the topic. Few grammar or spelling errors | Language is not precise or direct and doesn’t convey the information clearly. Multiple grammar and spelling errors | Language is irrelevant to the subject. |
| **Sequencing of Information** | Information is organized in logical manner. It is easy to follow the progression of topics | Most information is organized in a logical manner. | Some information is logically sequenced. | There is no clear plan for organization of information |

**Grading Sheet**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Category** | **Advanced (3)** | **Proficient (2)** | **Developing (1)** | **Not Demonstrated (0)** | **Total** |
| **Digital Identity Lifecycle** | **A, C** | **B** |  |  | 8 |
| **Authentication and Password Protection** | C | A | B |  | 6 |
| **Authorization** |  |  |  |  | /9 |
| **Accountability** |  |  |  |  | /9 |
| **Enterprise Identity Repository** |  |  |  |  | /9 |
| **Enterprise Password Policy Management** |  |  |  |  | /9 |
| **Access Control Management** |  |  |  |  | /9 |
| **Enterprise IDM and Integration** |  |  |  |  | /9 |
| **Privileged Access management** |  |  |  |  | /9 |
| **Data Ownership and Access Validation** |  |  |  |  | /9 |
| **Identity and Access Management Policy** |  |  |  |  | /9 |
| **Segregation of Duties and Job Rotation** |  |  |  |  | /9 |
| **Format** |  |  |  |  | /3 |
| **Language** |  |  |  |  | /3 |
| **Sequencing of Information** |  |  |  |  | /3 |
| **Total** | | | | | 117 |