# IT 6823 LM 1 Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

This module introduces students to the security field: it defines information security and explains how it different from cybersecurity and information assurance.

Given the technical nature of MSIT program, the course focus on the information security and cybersecurity.

## Student Learning Outcomes

* **Define Information Security**

“A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems”

Source: <https://csrc.nist.gov/glossary/term/security>

Information Assets: <https://csrc.nist.gov/glossary/term/asset>

* **Explain the difference among Information Security, information assurance, and cybersecurity**
1. *Information Security* – “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability”.

Source: <https://csrc.nist.gov/glossary/term/information_security>

1. *Information Assurance* – “Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities”.

Source: <https://csrc.nist.gov/glossary/term/information_assurance>

1. *Cybersecurity* – “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation”.

Source: <https://csrc.nist.gov/glossary/term/cybersecurity>

1. *Information Security vs. Cybersecurity:*
2. “The value of the data is the biggest concern for both types of security. In information security, the primary concern is protecting the confidentiality, integrity, and availability of the data. In cybersecurity, the primary concern is protecting unauthorized electronic access to the data. In both circumstances, it is important to understand what data, if accessed without authorization, is most damaging to the organization, so a security framework can be established with proper controls in place to prevent unauthorized access”.

Source: <https://securityscorecard.com/blog/information-security-versus-cybersecurity>

2) “While cyber security is about securing things that are vulnerable through Internet Communication Technology (ICT). It also considers that where data is stored and technologies used to secure the data. Part of cyber security about the protection of information and communications technologies – i.e. hardware and software, is known as ICT security”.



*Picture source: (*[*https://ccis.no/cyber-security-versus-information-security/*](https://ccis.no/cyber-security-versus-information-security/)*)*

Source: <https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information>

1. Information Security vs. Information Assurance

“Information Assurance is an activity organizations conduct to ensure that their systems protect private, sensitive information. Information Assurance is closely linked with risk management. An organization, such as a business, identifies its information assets and the systems and applications that store, process, and communicate them. It estimates the susceptibility of those information assets to attack, whether by disclosure (a loss of confidentiality), modification (a loss of integrity), or disruption (a loss of accessibility), and it quantifies the effect – usually in dollars – of those unwanted occurrences. From this, a risk assessment can guide an organization on how to devote personnel and capital resources optimally to protect its information. Once these protections are put in place, the practice of Information Assurance then calls for using various assessment and auditing frameworks to help an organization understand how well the controls it has deployed actually mitigate the risk.

Information Assurance specialists focus on the big business picture. They don’t concern themselves with operating systems kernels and the pitfalls of speculative instruction execution – the attack vector exploited by Meltdown, for example. Instead, Information Assurance experts seek to know how a company uses information, how valuable that information is to the company, and how exposed that information happens to be so that they can guide the organization on how to prioritize tasks to protect it. Once those protections are deployed by others, Information Assurance professionals help measure whether those protections are working.

Generally, Information Assurance professionals don’t focus as much in the actual design and deployment of those protections; they help decide what to protect and whether the protections are effective. They focus very much on the business. Indeed, an Information Assurance specialist could conduct all their work without ever having to bother about the esoteric details of bytes, protocols, and instruction registers. It’s all about information assets, valuations, optimization, strategy, and continuous assessment. It’s all about management, planning, auditing, and governance”.

Source: <https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/>

* **Describe the specialized areas of security**
1. Physical Security: It is to protect physical items, objects, or areas from unauthorized access and misuse
2. Personal Security: It is to protect the individual or group of individuals who are authorized to access the organization and its operations
3. Operation Security: It is to protect the details of the operation or a series of activities.
4. Communication Security: It is to communications media, technology, and content.
5. Network Security: It is to protect networking components, connections, and contents.
6. Information Security: it is the protection of information and its critical elements (Confidentiality, Integrity, and availability), including the systems and hardware that use, store, and transmit that information through the application of policy, education, technology, training, and awareness program.

Source: <https://sohail.life/3726/>

* **Describe the CIA Triad**
1. Confidentiality: Only authorized users and processes should be able to access or modify data
2. Integrity: Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously
3. Availability: Authorized users should be able to access data whenever they need to do so

Source: <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>

* **Define risks, threats, attacks and vulnerability**

Just need to understand the definition and major difference. Details will be covered in the risk management learning module.

Definitions can be found: <https://csrc.nist.gov/glossary>

Differences: <https://threatmodeler.com/differences-explained-threat-vs-vulnerability-vs-risk/>