# IT 6823 LM 2 Security Frameworks 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 mainly covers two major security frameworks: CNNS security model and NITS security framework. Those two frameworks give you a big picture about what information security is about. This module also introduces privacy, ethics, laws and regulations in information security.

## Student Learning Outcomes

* **Describe the CNNS security model and its applications**
1. Overview

National Security telecommunications & information systems security committee, now called the National Training Standard for Information Security Professional. The CNNS security model is a comprehensive model of InfoSec known as the McCumbers cube created in 1991, which is named after a developer, John McComber. It is becoming standard to determine the characteristics, location, and security of the information. It is a three-dimension model. These three dimensions are represented in a cube with 27 cells with each cell representing each aspect of information.

The cells that can be represented are the below

* + - Confidentiality, Integrity, availability
		- Policy, Education, Technology
		- Storage, Processing, Transmission

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

In 1991, John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, now known as The McCumber Cube.

Source: <https://en.wikipedia.org/wiki/McCumber_cube>



 Image source: <https://sohail.life/3726/>

1. Details of the model.

Details of the CNNS security model can be found in the PDF file in the D2L course site. Focus on page 22-28.

* **Discuss the NIST security framework**
1. Overview of the framework



Image source: <https://www.nist.gov/document/cybersecurityframeworkv1-1presentationpptx>

* Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
* Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
* Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
* Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
* Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Source: <https://doi.org/10.6028/NIST.CSWP.04162018>

1. Details of the framework

See the official document in PDF document in D2L course website. This is a long document. Concentrate on section 2. Framework Basics (page 13 – 18): main functions and implementation tiers.

* **Explain how to use NIST framework to review security practices**

Source: <https://doi.org/10.6028/NIST.CSWP.04162018> or the PDF file in D2L course website/LM2 (Page 20-21).

* **Describe how to establish or improve an information security program.**
1. Step 1: Prioritize and Scope.
2. Step 2: Orient
3. Step 3: Create a Current Profile
4. Step 4: Conduct a Risk Assessment.
5. Step 5: Create a Target Profile.
6. Step 6: Determine, Analyze, and Prioritize Gaps.
7. Step 7: Implement Action Plan.

An organization repeats the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

Source: <https://doi.org/10.6028/NIST.CSWP.04162018> or the PDF file in D2L course website/LM2 (Page 21-22).

* **Discuss the general security design principles**

Focus on the design principles list in this article: <https://docs.microsoft.com/en-us/azure/architecture/framework/security/security-principles>

* **Discuss the security and privacy**

Privacy relates to any rights you have to control your personal information and how it’s used. Think about those privacy policies you’re asked to read and agree to when you download new smartphone apps.

Security, on the other hand, refers to how your personal information is protected. Your data — different details about you — may live in a lot of places. That can challenge both your privacy and your security.

Some people regard privacy and security as pretty much the same thing. That’s because the two sometimes overlap in a connected world. But they aren’t the same, and knowing how they differ may help you to protect yourself in an increasingly connected world.

What’s the difference between privacy and security?

Here’s an example. You might share personal information with your bank when you open a checking account. What happens after that? Here are three possible outcomes, all related to your personal information (not to the money you may have deposited in the checking account).

* Your privacy and security are maintained. The bank uses your information to open your account and provide you with products and services. They go on to protect that data.
* Your privacy is compromised, and your security is maintained. The bank sells some of your information to a marketer. Note: You may have agreed to this in the bank’s privacy disclosure. The result? Your personal information is in more hands than you may have wanted.
* Both your privacy and security are compromised. The bank gets hit by a data breach. Cybercriminals penetrate a bank database, a security breach. Your information is exposed and could be sold on the dark web. Your privacy is gone. You could become the victim of cyber fraud and identity theft.

Source: <https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html>

* **Discuss the ethical issues and laws in information Security**
1. Ethical Issues for Information Security Professional
	* Deal with morals or the principles of morality; pertaining to right and wrong in conduct.
	* In accordance with the rules or standards for right conduct
	* Sometimes have a definitive answer
	* You determine your course of action
	* Rule-Based Ethics
	* Consequence-Based Ethics

Source: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiUoMv4h-jtAhUEx1kKHTIsA44QFjADegQIBBAC&url=http%3A%2F%2Fkhabib.staff.ugm.ac.id%2Fdownloads%2Flecture%2FITAudit%2Flegal-ethic.pdf&usg=AOvVaw3LP-RonQOwp3U2wNbkwgRT>

1. Laws and Regulations (Just needs to know what those laws are. Don’t need to know the details).
* [Privacy Act of 1974](https://www.justice.gov/opcl/privacy-act-1974)
* [Computer Security Act of 1987](https://www.congress.gov/bill/100th-congress/house-bill/145)
* [Computer Fraud and Abuse Act (CFAA)](https://www.nacdl.org/Landing/ComputerFraudandAbuseAct)
* [Family Educational Rights and Privacy Act (FERPA)](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
* [Health Insurance Portability and Accountability Act (HIPAA)](https://www.cdc.gov/phlp/publications/topic/hipaa.html)