# LM 10. Incident Response and Recovery

### Overview

The module gives an overview of incident response and recovery.  The learning material is mainly based on NIST publication SP 800-61 Rev. 2 which provided in the D2L course website as a PDF file. The document is referred as “SP 800-61” in the rest of this document. SP 800-61 is available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Incident response and recovery is response phase in the NITS security framework.

### To Do List

* 1. Study the learning material of this module - security frameworks. Use the learning material document and PowerPoint slides as a guide.
  2. Complete LM10 discussion - analyze an incident response scenario. Must be completed by **xx.** The initial post needs to be made by xx to qualify for full credit.

### Learning Outcomes

After this module, student will be able to:

* Discuss the need for incident response
* Describe the elements of incident response policy
* Discuss the incident response team structure
* Explain the incident response life cycle
* Discuss the coordination and information sharing