

# Glossary terms from module 1

## Terms and definitions from Course 5, Module 1

**Asset:** An item perceived as having value to an organization

**Asset classification:** The practice of labeling assets based on sensitivity and importance to an organization

**Asset inventory:** A catalog of assets that need to be protected

**Asset management:** The process of tracking assets and the risks that affect them

**Compliance:** The process of adhering to internal standards and external regulations

**Data:** Information that is translated, processed, or stored by a computer

**Data at rest:** Data not currently being accessed

**Data in transit:** Data traveling from one point to another

**Data in use:** Data being accessed by one or more users

**Information security (InfoSec):** The practice of keeping data in all states away from unauthorized users

**National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

**Policy:** A set of rules that reduce risk and protect information

**Procedures:** Step-by-step instructions to perform a specific security task

**Regulations:** Rules set by a government or other authority to control the way something is done

**Risk:** Anything that can impact confidentiality, integrity, or availability of an asset

**Standards:** References that inform how to set policies

**Threat:** Any circumstance or event that can negatively impact assets

**Vulnerability:** A weakness that can be exploited by a threat