14.2.4 Security Frameworks Facts

This lesson covers the following topics:

- Laws, regulations, and compliance
- Security frameworks
- Cloud security

Laws, Regulations, and Compliance

Compliance with local, national, and international security regulations and laws is now part of daily operations. These requirements cover close to all data that is collected, used, stored, and shared. These requirements have many variables that include but are not limited to: industry, size of company, types of PII, and the use of data.

Substantial financial penalties are levied when a company is found non-compliant. The services of legal advisors is highly recommended to ensure compliance. The two most important laws in recent memory are the GDPR, or the General Data Protection Regulation of the European Union, and the California Consumer Protection Act

Security Frameworks

Security frameworks provide a guide or roadmap to compliance requirements. In many instances, the framework provides various levels of compliance. These levels often correspond with the size of government.

Security Framework	Description
NIST	The National Institute of Standards and Technology (NIST) is one of the largest security frameworks. It is used by the federal government and all its departments, including the Department of Defense. Security is one of the many verticals that NIST provides guidance for, and NIST's cybersecurity frameworks are the gold standard in our business.
ISO	The International Organization for Standardization (ISO) is a worldwide organization that is currently the standardizing body in 164 different countries. Publication available are: ▪ ISO 27001 is the publication that covers implementing and improving a security management system as well as an assessment guideline. ▪ Publication 27002 lays out guidelines for selecting and implementing security controls. ▪ NIST 31000 covers risk management as it pertains to business continuity, safety, environmental results, and the professional reputation of a company. ▪ ISO 27701 covers establishing, implementing, and improving a privacy information management system. This is geared towards companies that need to comply with privacy laws and regulations.
SOC Type II/III	The System and Organization Controls (SOC) has three types of reports that help a third party determine (through an audit) how a company is adhering to systems and controls. The types of SOC reports we will discuss are Type II and Type III. ▪ Type II reports focus on predetermined controls that are audited and a detailed report that attests to the company's compliance. It is a non-financial report and it relates to

	processing, integrity, security, availability, confidentiality, and network privacy. ▪ Type III is a non-detailed report attesting to the company's compliance. This type of report is used for marketing and letting future partners know that compliance has been met.

Cloud Security

The Cloud Security Alliance (CSA) is a relatively new, ten-year-old security framework. With the exponential growth of cloud computing, the need for a cloud security framework was crucial.

Along with best practices in cloud security, CSA also introduced the first cloud-centric individual certification. It works because it aggregates best security practices from all business and educational verticals. This ensures that the individual framework needs of each company are met using relevant, up-to-date information.

Within CSA, there is a Cloud Control Matrix (CCM). This matrix is a guide to assist prospective cloud users in evaluating a cloud provider's security risk. This matrix also helps cloud providers integrate fundamental security principles into their services. It works with frameworks like NIST, ISO 27001, and ISO 27002. The function of CSA and CCM are:

- CSA
  - Provides cloud security framework
  - Compiles best practices
- Cloud Control Matrix
  - Provides security guide for cloud users
  - Works with major security frameworks

It is important that, as a security professional, you keep current with changes to laws, regulations, and frameworks.