Note: The reviews is based of Shon Harris’ book “All in One CISSP Exam Guide fifth edition” some phrases are taken verbatim from Shon Harris book (especially but not including phrases in quotes) for the purpose of a review summary.

Chapter 10: Legal, Regulations, Compliance and Investigations Summary:

* Computer assisted crime: a crime in which a computer is used to commit the crime
* Computer –targeted crime: When a computer system is the target of a crime
* Computer incidental: when a computer system may be involved but the computer does not play a significant role in the crime.
  + Example: computer disks are stolen from a company, and those disks are read on a computer.
* Script kiddie – a person who doesn’t not know how to “hack” but uses tools that others write to break into systems.
* Trade Secret – information that belongs to a company and is crucial to it’s success or provides competitive advantages.
* Copyright – “protects the right of an author to control the public distribution, reproduction, display and adaptation of their original work”, protects the expressions of idea. “Can be applied to writing, drawing, art etc”
* Trademark – “protects a workd, name, symbol etc that expresses a brand or companies identity”
  + Cannot trademark a common word, or number.
* Patent – protects intellectual property. Protects inventions or new ideas to solve problems”
* Freeware – software made available for free
* Shareware / trialware – free “demo” software, providing some set of functionality (or time limit) that can be unlocked for a fee.
* The European Union is more concerned about **privacy** concerns than most other countries.
* Software piracy – the illegal use and or distribution of commercial software.

Types of Law (page 857-858):

* Civil Law – rule based, not precedence based
* Common Law – based on previous interpretations of laws, customs and precedence.
  + Uses a jury of peers
  + Two types
    - Criminal – behavior considered harmful to society, person is responsible to the court/penalty system
    - Civil/tort – a person is responsible to another individual (penalties are financial) (burden of proof requirement is lower than Criminal law)
* Religious Law – Law is based on religious beliefs and rules
* Mixed Law – Systems that are hybrids of the above systems.
* Software Protection Association (SPA) – an organization formed by major companies to fight software piracy.
* Digital Millennium Copyright Act (DMCA) – a law making it illegal to create products that circumvent copyright protection.
* Sarbanes Oxley Act (SOX) – concerned with publically traded companies, creates rules regarding accounting and auditing practices. Impacts IT systems.
* Health Insurance Portability and Accounting Act – Concerned with privacy of personal health records.
* Gramm-Leach-Bliley Act of 1999 – requires financial institutions to develop privacy notices and allow individuals to prohibit the sharing of information with 3rd parties.
* The Computer Fraud and Abuse Act – primary federal anti-hacking law.
* Federal Privacy Act of 1974 – states that a government agency can collect information on individuals , however the
  + information gathered must be “relevant and necessary”, information
  + the information cannot be shared, without written permission of the individual
  + violations allow the individual to sue the government
* Computer Security act of 1987 – US agencies must identify computer systems with sensitive information and develop a security policy for those systems.
* Economic Espionage Act of 1996 – allows the FBI to investigate incidences of espionage.
* Basel II – “concerned with protecting banks from overextending themselves and becoming insolvent.”.
  + Based on 3 main components “pillars” (minimum capital requirements, supervision, and market discipline)
  + Not a law
* PCI-DSS – concerned with ensuring safety and security of credit card processing.
  + Familiarize yourself with the 12 requirements
  + Not a law.
* Employee Privacy Issues – monitoring of users is allowed if the locality permits it, however
  + monitoring must be related to work and
  + monitoring must be applied consistently
  + employees must be notified of potential monitoring

**Thoroughly read pages 879 – 903 all the terms and ideas there are important for the exam, do not skim this section. Read it and understand it thoroughly. Everything in these pages is relevant and important to the exam, such that I am not going to even try to summarize it. Read it and understand it ALL.**

* Salami attack – an attacker performs a series of small crimes that amount to a large crime. Such as stealing $.01 from every transaction in a banking system.
* Data Diddling – altering data to commit a crime.
* Sniffing – reading network information as it goes across a wire (usually un-encrypted)
* IP spoofing – forging an IP address
  + Use ingress and egress filtering to stop IP spoofing
* Dumpster Diving – social engineering attack where a attacker goes through trash to find important information.

Ethics

* Know the 10 commandments of the Computer Ethics Institte
* Internet Architecture Boards – the IAB is most concerned with wasting Internet resources / disrupting Internet resources